Ruckus Wireless™ ZoneFlex™ Indoor Access Point

Release 9.3 User Guide

For the following indoor ZoneFlex AP models:

- ZoneFlex 2942 802.11g Access Point
- ZoneFlex 7942 802.11n Access Point
- ZoneFlex 7962 Dual Band 802.11n Access Point
- ZoneFlex 7341 802.11n Smart Wi-Fi Access Point
- ZoneFlex 7343 802.11n Smart Wi-Fi Access Point
- ZoneFlex 7363 Dual Band 802.11n Smart Wi-Fi Access Point

Part Number 800-70355-001
Published December 2011

www.ruckuswireless.com

Contents

About This Guide

Document Conventions i
Related Documentation ii
Documentation Feedback ii

1 Introducing the ZoneFlex Access Point

Overview of the ZoneFlex Access Point 1
Unpacking the ZoneFlex Access Point 2
Package Contents 2
Getting to Know the Access Point Features 2
ZoneFlex 2942/7942 Access Point 3
ZoneFlex 7962 Access Point 7
ZoneFlex 7341 Access Point 11
ZoneFlex 7343 Access Point 13
ZoneFlex 7363 Access Point 17

2 Installing the Access Point

Before You Begin 21
Prepare the Required Hardware and Tools 21
Perform a Site Survey 22
Determine the Optimal Mounting Location and Orientation 23
Step 1: Preconfigure the Access Point 28
Configuring for Management by ZoneDirector 28
Configuring for Standalone Operation or for Management by FlexMaster 30
Step 2: Verify Access Point Operation 37
Connect the Access Point to the Network 37
Associate a Wireless Client with the Access Point 37
Check the LEDs 38
Check the TR069 Status (FlexMaster Management Only) 38
Disconnect the Access Point from the Network 39
Step 3: Deploy the Access Point 40

1. Choose a Location for the Access Point 40
2. Connect the Access Point to a Power Source and the Network 40
Troubleshooting Installation 41

3 Navigating the Web Interface

Logging Into the ZoneFlex Web Interface. 43
Navigating the Web Interface. 44
If You Are Using a Dual Band ZoneFlex Access Point. 45

4 Configuring the Access Point

Configuring Device Settings 48
Configuring Internet Settings 49
VLAN Settings Overview 49
Configuring NTP Server and Management VLAN 50
Default IP Addressing Behavior 50
Obtaining and Assigning an IP Address 51
Configuring L2TP Connection Settings 53
Configuring Local Subnets 55
Configuring Wireless Settings. 56
Configuring Common Wireless Settings 56
Configuring Wireless # Settings 62
Configuring Ethernet Ports 75
Setting Ethernet Port Type 77
Working with 802.1X on Wired Ethernet Ports 78
Working with Port-Based VLANs 80
Configuring Hotspot Service. 80
Customizing Hotspot Optional Settings 82
Creating a Hotspot Walled Garden 84
Allowing Unrestricted Access by MAC Address 85

5 Managing the Access Point

Viewing Current Device Settings 88
Viewing Current Internet Connection Settings 89
Viewing Current Local Subnet Settings 90
Viewing Current Wireless Settings 91

Viewing Associated Wireless Clients 92
Changing the Administrative Login Settings. 93
Enabling Other Management Access Options 94
Viewing FlexMaster Management Status 98
Pointing the AP to FlexMaster 99
Working with Event Logs and Syslog Servers 100
Enabling Logging and Sending Event Logs to a Syslog Server 100
Sending a Copy of the Log File to Ruckus Wireless Support 101
Saving a Copy of the Current Log to Your Computer 101
Upgrading the Firmware 102
Upgrading Manually via FTP or TFTP 102
Upgrading Manually via the Web 103
Upgrading Manually via Local File 103
Scheduling Automatic Upgrades 103
Rebooting the Access Point 104
Resetting the Access Point to Factory Defaults. 105
Running Diagnostics 106
Where to Find More Information 108

Index

About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless™ ZoneFlex™ Access Point. This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE: If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at: http://support.ruckuswireless.com/

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text Conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
	Information	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Related Documentation

In addition to this User Guide, each ZoneFlex Access Point documentation set includes the following:

- *Quick Start Guide*: Provides essential installation and configuration information to help you get the AP up and running within minutes.
- *Online Help*: Provides instructions for performing tasks using the Access Point's Web interface. The online help is accessible from within the Web interface.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

NOTE: If you will be managing your ZoneFlex Access Points using ZoneDirector, refer to the ZoneDirector User Guide (available from the Ruckus Wireless website).

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus Wireless ZoneFlex Indoor Access Point Release 9.3 User Guide
- Part number: 800-70355-001
- Page 88

1

Introducing the ZoneFlex Access Point

In This Chapter

Overview of the ZoneFlex Access Point 1
Unpacking the ZoneFlex Access Point 2
Getting to Know the Access Point Features 2

Overview of the ZoneFlex Access Point

Congratulations on your purchase of the Ruckus Wireless ZoneFlex Access Point! ZoneFlex Access Points are the industry's most easy to use, yet robust and feature-rich Wi-Fi Access Points designed to bring power and simplicity together for large-scale indoor deployments.

Your ZoneFlex Access Point uses BeamFlex™, a patented antenna technology from Ruckus Wireless that allows wireless signals to navigate around interference, extend wireless signal range, and increase speeds and capacity for wireless networks. The BeamFlex™ antenna system consists of an array of up to fourteen high-gain directional antenna elements that allow ZoneFlex Access Points to find quality signal paths in a changing environment, and sustain the baseline performance required for supporting data, audio and video applications.

Your ZoneFlex Access Point can be deployed in standalone mode or as part of the ZoneFlex Smart WLAN system, in which it can be managed by either FlexMaster or ZoneDirector WLAN controller.

NOTE: For more information on the ZoneFlex system (including FlexMaster and ZoneDirector), BeamFlex, and other Ruckus Wireless technologies, visit www.ruckuswireless.com.

Unpacking the ZoneFlex Access Point

1. Open the Access Point package, and then carefully remove the contents.
2. Return all packing materials to the shipping box, and put the box away in a dry location.
3. Verify that all items listed in Package Contents below are included in the package. Check each item for damage. If any item is damaged or missing, notify your authorized Ruckus Wireless sales representative.

Package Contents

A complete Access Point package contains all of the items listed below:

- ZoneFlex Access Point
- Software License Agreement/Product Warranty Statement
- Quick Setup Guide
- *(Ethernet cables, power adapters and mounting kits are optional accessories that may or may not be included depending on the SKU purchased)*

Getting to Know the Access Point Features

This section identifies the physical features of each ZoneFlex Access Point model that is discussed in this guide. Before you begin the installation process, Ruckus Wireless recommends that you become familiar with these features.

- ZoneFlex 2942/7942 Access Point
- ZoneFlex 7962 Access Point
- ZoneFlex 7341 Access Point
- ZoneFlex 7343 Access Point
- ZoneFlex 7363 Access Point

NOTE: This User Guide does not include information on ZoneFlex Outdoor Access Points, ZoneFlex 7731 Wireless Bridge, or ZoneFlex 7025 Multimedia Wi-Fi Wall Switch. For information on those ZoneFlex models (along with Ruckus Wireless MediaFlex and MetroFlex product lines), refer to their respective documentation available from support.ruckuswireless.com.

ZoneFlex 2942/7942 Access Point

The side panel of ZoneFlex 2942/7942 features four LED indicators that can be used to assess both device and network status. The rear view displays the connector panel, which includes the LAN ports and the optional external antenna connection. Refer to the following illustrations and tables to learn more.

Side Panel Features

The ZoneFlex 2942/7942 chassis includes a Kensington lock (on the side of the unit opposite the OPT and DIR LEDs) and a lockable "sliding door" (shown in Figure 1) that hides and protects the rear connector I/O panel and status LEDs. As your AP may be placed in a public location, the lock and door mechanisms can help prevent tampering or theft.

Figure 1. ZoneFlex 2942/7942 side panel features

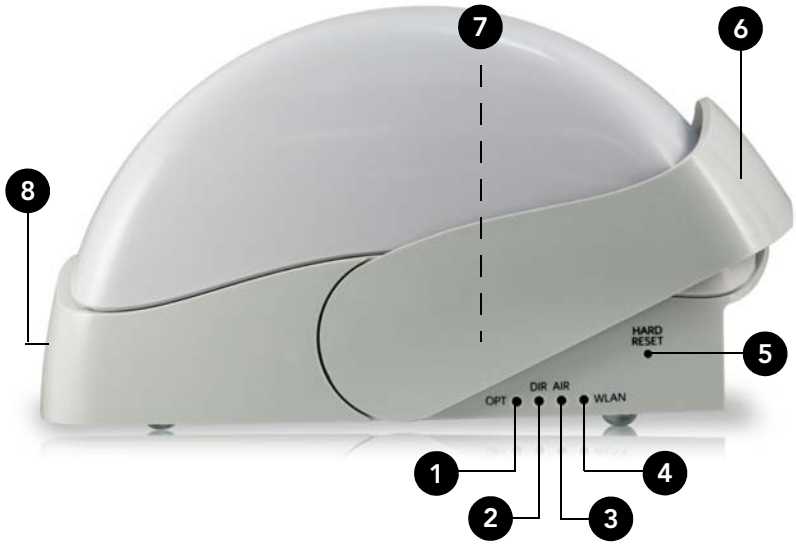


Table 3 lists the various LED states on ZoneFlex 2942/7942 and describes what each LED state means. It also describes how to use the HARD RESET button and other elements on the side panel.

Table 3. ZoneFlex 2942/7942 side panel elements

Number	LED/Button Name	Description
1	OPT LED	Not used in this model

Table 3. ZoneFlex 2942/7942 side panel elements

Number	LED/Button Name	Description
2	DIR LED	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Slow flashing green (one flash every two seconds):* The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green (two flashes every second):* The Access Point is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.
3	AIR LED	• *Off*: The WLAN service is down. • *Green*: The AP is functioning as a Root AP (RAP) or Mesh AP (MAP), and the uplink signal is *good*. • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the AP is still searching for a mesh uplink. • *Fast flashing green (two flashes every second)*: The Access Point is functioning as a Mesh AP and the wireless signal to its uplink AP is *fair*.
4	WLAN LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients are associated and no downlink MAPs are connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green (one flash every two seconds)*: The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green (two flashes every second)*: The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.
5	HARD RESET Button	Pushing and quickly releasing this button reboots the AP. Pushing and holding it for six seconds resets the AP to factory defaults.
6	Sliding Door	Protects the ports, buttons, and connector on rear panel

Table 3. ZoneFlex 2942/7942 side panel elements

Number	LED/Button Name	Description
7	Kensington Lock	The Kensington lock feature, located on the opposite side of the unit from the pictured LEDs, is designed to prevent the sliding door from opening, thus locking the unit. The Kensington lock works with a Kensington MicroSaver lock.
8	Power LED (front)	• *Off*: Off • *Red*: Boot up in process • *Green*: On

Rear Panel Features

Figure 2 shows the rear panel of ZoneFlex 2942/7942. For a description of each rear panel part, refer to Table 4.

Figure 2. ZoneFlex 2942/7942 rear panel features

WARNING: *For units with Power over Ethernet (PoE).* These products and all interconnected equipment must be installed indoors within the same building, including the associated LAN connections, as defined by Environment A of the IEEE 802.3af Standard.

CAUTION: The external antenna connectors are for indoor use only. Do not connect them to outdoor antennas.

Table 4. ZoneFlex 2942/7942 rear panel elements

Number	Item Name	Description
1	Power	Connect the power adapter to this socket. (Input 110-240V AC, Output 12V 1.0A DC). Power can also be supplied via 10/100 PoE port.
2	Lock Hasp	The lock hasp works with a cable or Ruckus mounts. The recommended lock type is Masterlock 120 series (D, T, Q, KAD types).
3	External RP-SMA Connector	• ZoneFlex 2942: One external antenna connector • ZoneFlex 7942: None
4	LAN Ports	• ZoneFlex 2942: Two RJ-45 ports, supporting 10/100 PoE (Power over Ethernet) and 10/100Mbps connections. • ZoneFlex 7942: Two RJ-45 ports, supporting 10/100/1000 PoE (Power over Ethernet) and 10/100/1000Mbps connections. Each Ethernet port has two LEDs, which indicate the type of device that is connected to the port.
5	OPTIONAL Button	Not active in this model at this time.
6	SOFT RESET Button	Used to reset the AP. This is a normal reset and does not reset the AP back to factory defaults.

Table 5. Behavior of Ethernet port LEDs on ZoneFlex 2942/7942

LEDs	Description
Off	Not connected
Steady flashing Amber + Green	Connected to 10Mbps device
Steady flashing Amber	Connected to 100Mbps device
Steady flashing Green	Connected to 1000Mbps device
Intermittent flashing Amber + Green	Connected to 10Mbps device, and passing traffic
Intermittent flashing Amber	Connected to 100Mbps device, passing traffic
Intermittent flashing Green	Connected to 1000Mbps device, passing traffic

ZoneFlex 7962 Access Point

The physical features of ZoneFlex 7962 are very similar to ZoneFlex 2942/7942. It uses the same dome-type chassis with the sliding door and Kensington lock on the side panel. There are slight differences, however, in the side panel and rear panel elements. Refer to the illustrations below for more information.

Side Panel Features

Figure 3 illustrates the side panel features of ZoneFlex 7962. For a description of each rear panel part, refer to Table 6.

Figure 3. ZoneFlex 7962 side panel

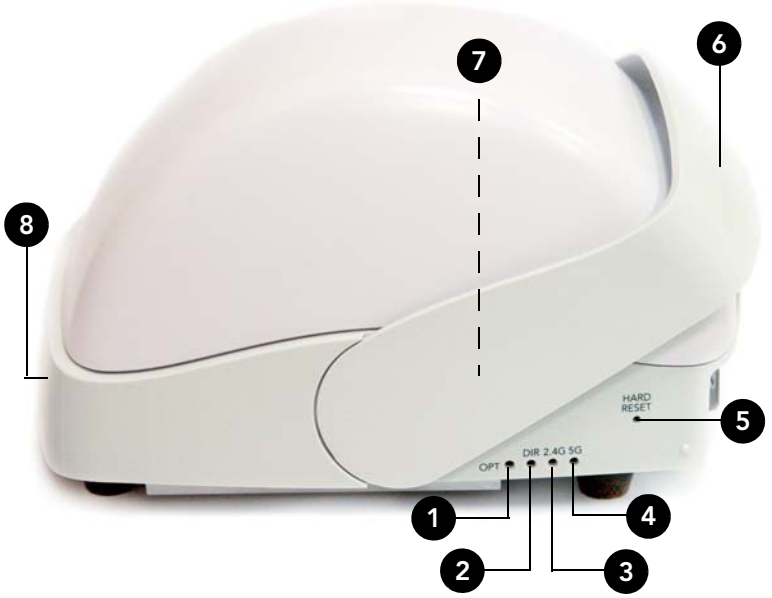


Table 6. ZoneFlex 7962 side panel elements

Number	LED/Button Name	Description
1	OPT LED	Not used in this model

Table 6. ZoneFlex 7962 side panel elements

Number	LED/Button Name	Description
2	DIR LED	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Slow flashing green (one flash every two seconds):* The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green (two flashes every second):* The Access Point is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.
3	2.4G LED (WLAN)	• *Off*: The WLAN service is down. • *Amber*: The WLAN service is up, at least one wireless client is associated (standalone), or at least one downlink MAP is connected (RAP), or uplink RAP is connected (MAP), but signal quality is *poor* (RSSI < 15). • *Green*: The WLAN service is up, at least one client is associated (standalone), or at least one downlink MAP is connected (RAP), or uplink RAP is connected (MAP), and signal quality is *good* (RSSI >= 15). • *Flashing green*: The WLAN service is up, no clients are associated (standalone), no downlink MAPs are connected (RAP), or no uplink RAP is connected (MAP).
4	5G LED (WLAN)	• *Off*: The WLAN service is down. • *Green*: The WLAN service is up and at least one wireless client is associated. • *Fast flashing green (two flashes every second)*: The WLAN service is up and no wireless clients are associated. • *Slow flashing green*: zMesh AP searching for an uplink, or searching for ZoneDirector.

Table 6. ZoneFlex 7962 side panel elements

Number	LED/Button Name	Description
5	HARD RESET Button	Pushing and quickly releasing this internal button reboots the AP. Pushing and holding it for six seconds resets the AP to factory default settings. CAUTION! Resetting the AP to factory default settings will erase all settings that you configured previously.
6	Sliding Door	Protects the ports, buttons, and connector on the rear panel
7	Kensington Lock	The Kensington lock feature, located on the opposite side of the unit from the pictured LEDs, is designed to prevent the sliding door from opening, thus locking the unit. The Kensington lock works with a Kensington MicroSaver lock.
8	Power LED (front)	• *Off*: Off. • *Amber*: Boot up in process. • *Green*: On.

Rear Panel Features

Figure 4 shows the rear panel of ZoneFlex 7962. For a description of each rear panel part, refer to Table 7.

Figure 4. ZoneFlex 7962 rear panel features

Table 7. ZoneFlex 7962 rear panel elements

Number	Item Name	Description
1	Power	Connect the power adapter to this socket. (Input 110-240V AC, Output 12V 1.0A DC). Power can also be supplied via the 10/100/1000 PoE port.
2	Lock Hasp	The lock hasp works with a cable or Ruckus Wireless mounts. The recommended lock type is Masterlock 120 series (D, T, Q, KAD types).
3	LAN Ports	Two RJ-45 ports, one for a 10/100/1000 PoE (Power over Ethernet) connection and another for a 10/100/1000Mbps connection. Each Ethernet port has two LEDs, which indicate the type of device that is connected to the port. • Flashing green + amber: 10Mbps Layer 2 device • Flashing amber: 100Mbps Layer 2 device • Flashing green: 1000Mbps Layer 2 device

Table 7. ZoneFlex 7962 rear panel elements

Number	Item Name	Description
4	OPTIONAL Button	Not active in this model at this time.
5	SOFT RESET Button	Use to reset AP. This is a normal reset and does not set AP back to factory defaults.

ZoneFlex 7341 Access Point

ZoneFlex 7341 features five LEDs on its front panel, and buttons and connectors on its rear panel.

Front Panel

Figure 5 shows the front panel of ZoneFlex 7341. For a description of each front panel part, refer to Table 8.

Figure 5. ZoneFlex 7341 front panel

Table 8. ZoneFlex 7341 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model

Table 8. ZoneFlex 7341 front panel elements

LED	Description
DIR LED	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The Access Point is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.
WLAN LED	• *Off*: The WLAN service is down. • *Amber:* The WLAN service is up and no clients are associated (standalone), or no wireless clients and no downlink MAPs are connected (RAP). • *Green*: The WLAN service is up and at least one wireless client is associated. If Mesh is enabled, no downlink MAPs are connected. • *Fast flashing green*: The WLAN service is up, at least one client is associated, and at least one Mesh downlink is connected. • *Slow flashing green*: At least one Mesh downlink is connected, and no clients are associated.
AIR LED	• *Off*: The WLAN service is down. • *Green*: The AP is functioning as a RAP or MAP and the uplink signal is *good*. • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the AP is still searching for a mesh uplink. • *Fast flashing green (two flashes every second)*: The AP is functioning as a MAP and the wireless signal to its uplink AP is *fair*.

Rear Panel

Figure 6 shows the rear panel of ZoneFlex 7341. For a description of each rear panel part, refer to Table 9.

Figure 6. ZoneFlex 7341 rear panel

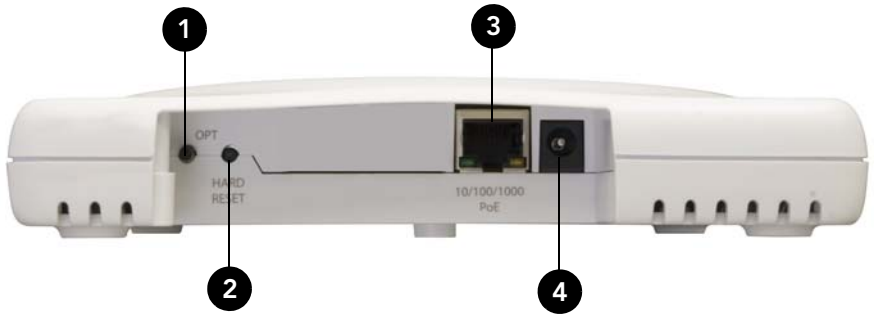


Table 9. ZoneFlex 7341 rear panel elements

Number	Item Name	Description
1	OPT Button	Not active in this model at this time.
2	HARD RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. *CAUTION! Resetting the AP to factory default settings will erase all settings that you configured previously.*
3	10/100/1000 PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
4	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE (802.3af) port.

ZoneFlex 7343 Access Point

ZoneFlex 7343 features five LEDs on its front panel, and buttons and connectors on its rear panel.

Front Panel

Figure 7 shows the front panel of ZoneFlex 7343. For a description of each front panel part, refer to Table 10.

Figure 7. ZoneFlex 7343 front panel

Table 10. ZoneFlex 7343 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model
DIR LED	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The Access Point is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.

Table 10. ZoneFlex 7343 front panel elements

LED	Description
WLAN LED	• *Off*: The WLAN service is down. • *Amber:* The WLAN service is up and no clients are associated (standalone), or no wireless clients and no downlink MAPs are connected (RAP). • *Green*: The WLAN service is up and at least one wireless client is associated. If Mesh is enabled, no downlink MAPs are connected. • *Fast flashing green*: The WLAN service is up, at least one client is associated, and at least one Mesh downlink is connected. • *Slow flashing green*: At least one Mesh downlink is connected, and no clients are associated.
AIR LED	• *Off*: The WLAN service is down. • *Green*: The AP is functioning as a RAP or MAP and the uplink signal is *good*. • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the AP is still searching for a mesh uplink. • *Fast flashing green (two flashes every second)*: The AP is functioning as a MAP and the wireless signal to its uplink AP is *fair*.

Rear Panel

Figure 8 shows the rear panel of ZoneFlex 7343. For a description of each rear panel part, refer to Table 11.

Figure 8. ZoneFlex 7343 rear panel

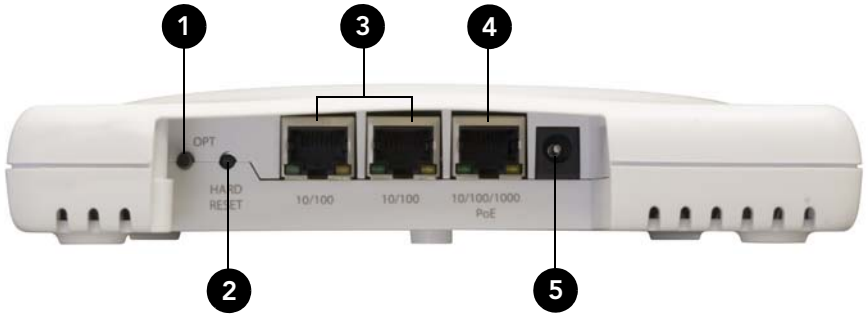


Table 11. ZoneFlex 7343 rear panel elements

Number	Item Name	Description
1	OPT Button	Not active in this model at this time.
2	HARD RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. *CAUTION! Resetting the AP to factory default settings will erase all settings that you configured previously.*
3	10/100 Ports (2)	Two RJ-45 ports for 10/100Mbps connections.
4	10/100/1000 PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
5	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE (802.3af) port.

ZoneFlex 7363 Access Point

ZoneFlex 7363 features five LEDs on its front panel, and buttons and connectors on its rear panel.

Front Panel

Figure 9 shows the front panel of ZoneFlex 7363. For a description of each front panel part, refer to Table 12.

Figure 9. ZoneFlex 7363 front panel

Table 12. ZoneFlex 7363 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Amber*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.

Table 12. ZoneFlex 7363 front panel elements

LED	Description
2.4G LED (WLAN)	• *Off*: The WLAN service is down. • *Amber*: The WLAN service is up, at least one wireless client is associated (standalone), or at least one downlink MAP is connected (RAP), or uplink RAP is connected (MAP), but signal quality is *poor* (RSSI < 15). • *Green*: The WLAN service is up, at least one client is associated (standalone), or at least one downlink MAP is connected (RAP), or uplink RAP is connected (MAP), and signal quality is *good* (RSSI >= 15). • *Flashing green* (two flashes every second): The WLAN service is up but no clients are associated (standalone), no downlink MAPs are connected (RAP), or no uplink RAP is connected (MAP).
5G LED (WLAN)	• *Off*: The WLAN service is down. • *Amber:* The WLAN service (or mesh network) is up and at least one wireless client is associated, but RSSI is *low*. If mesh networking is enabled, at least one downlink MAP is connected. • *Green*: The wireless WLAN service (or mesh network) is up and at least one wireless client is associated. If mesh networking is enabled, at least one downlink MAP is connected. • *Fast flashing green (two flashes every second)*: The WLAN service (or mesh network) is up, but no wireless clients or downlink MAPs are currently associated. • *Slow flashing green (one flash every two seconds)*: The WLAN service is up, no wireless clients are currently associated, mesh networking is enabled and at least one downlink MAP is connected.

Rear Panel

Figure 10 shows the rear panel of ZoneFlex 7363. For a description of each rear panel part, refer to Table 13.

Figure 10. ZoneFlex 7363 rear panel

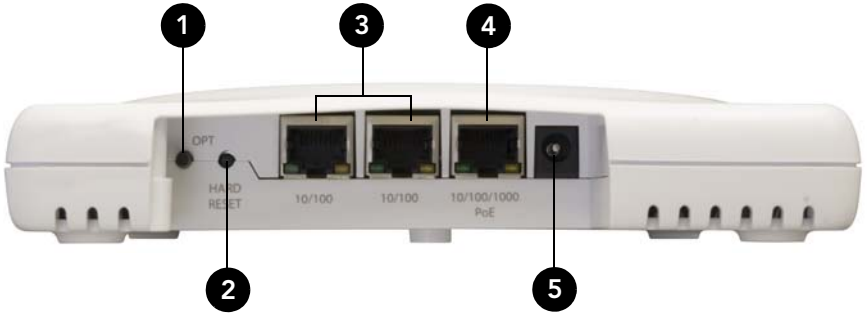


Table 13. ZoneFlex 7363 rear panel elements

Number	Item Name	Description
1	OPT Button	Not active in this model at this time.
2	HARD RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. *CAUTION! Resetting the AP to factory default settings will erase all settings that you configured previously.*
3	10/100 Ports (2)	Two RJ-45 ports for 10/100Mbps connections
4	10/100/1000 PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection
5	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE (802.3af) port.

2

Installing the Access Point

In This Chapter

Before You Begin 21
Step 1: Preconfigure the Access Point 28
Step 2: Verify Access Point Operation 37
Step 3: Deploy the Access Point 40
Troubleshooting Installation 41

Before You Begin

Before starting with the installation, make sure that you have the required items for the installation ready. In addition, verify that the wireless stations on the network have the required components for wireless communication with the Access Point.

This section describes the pre-installation tasks that you need to perform.

Prepare the Required Hardware and Tools

You must supply the following tools and equipment:

- A notebook computer running Windows (2000/XP/Vista/7) with one wireless 802.11a/b/g/n network card and one Ethernet card installed
- A modem (DSL or cable), E1/T1 router, or other device provided by your Internet Service Provider, that brings Internet access to your site
- (Optional) A network switch or a DSL/Internet gateway device.

NOTE: If the AP is deployed with ZoneDirector, follow the instructions in the *ZoneDirector Quick Setup Guide*, and connect the AP to your Ethernet network.

Perform a Site Survey

Before installing the Access Point, perform a site survey to determine the optimal Access Point placement for maximum range, coverage, and network performance. When performing a site survey, consider the following factors:

- *Data rates*: Range is generally inversely proportional to data rates. The maximum radio range is achieved at the lowest workable data rate. Higher data rates will generally be achieved at closer distances.
- *Antenna type and placement*: Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, radio range is increased by mounting the antennas higher off of the ground.
- *Physical environment*: Clear or open areas provide better radio range than closed or filled areas. The less cluttered the operating environment, the greater the wireless range.
- *Obstructions, building materials, and sources of interference*: Physical obstructions, such as concrete pillars, steel beams and filing cabinets can block or hinder wireless communication. Avoid installing the Access Point in a location where there is an obstruction between sending and receiving devices. A number of machines and electronic devices that emit radio waves – cranes, wireless phones, microwave ovens, satellite dishes – interfere with and block wireless signals. Building materials used in construction also influence radio signal penetration. For example, drywall construction permits greater range than concrete blocks.

For more Access Point placement guidelines, refer to "Determine the Optimal Mounting Location and Orientation".

Determine the Optimal Mounting Location and Orientation

The location and orientation that you choose for the Access Point play a critical role in the performance of your wireless network. In general, Ruckus Wireless recommends installing the Access Point away from obstructions and sources of interference and ensuring that the top of the Access Point is pointing in the general direction of its wireless clients.

The recommended orientation differs slightly depending on the Access Point model. See the following sections according to your particular model:

- ZoneFlex 2942, 7942, 7962 Orientation
- ZoneFlex 7341, 7343 and 7363 Orientation

ZoneFlex 2942, 7942, 7962 Orientation

Figure 11. Recommended orientation for maximum horizontal plane coverage

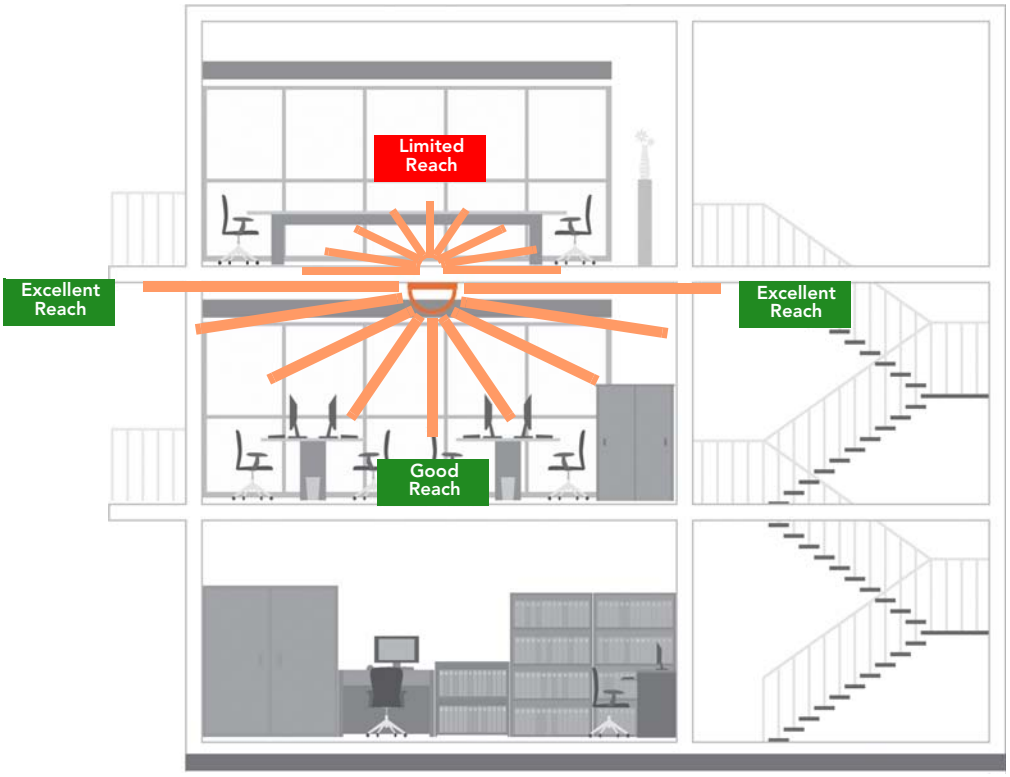


Figure 12. Recommended orientation for maximum vertical plane coverage

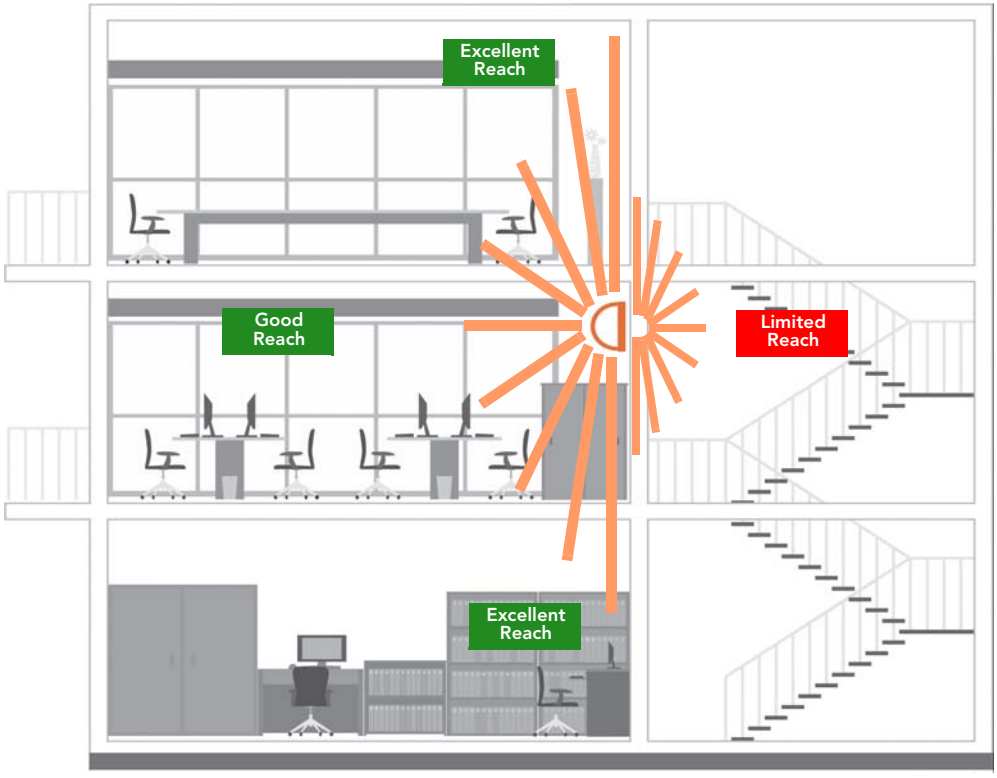
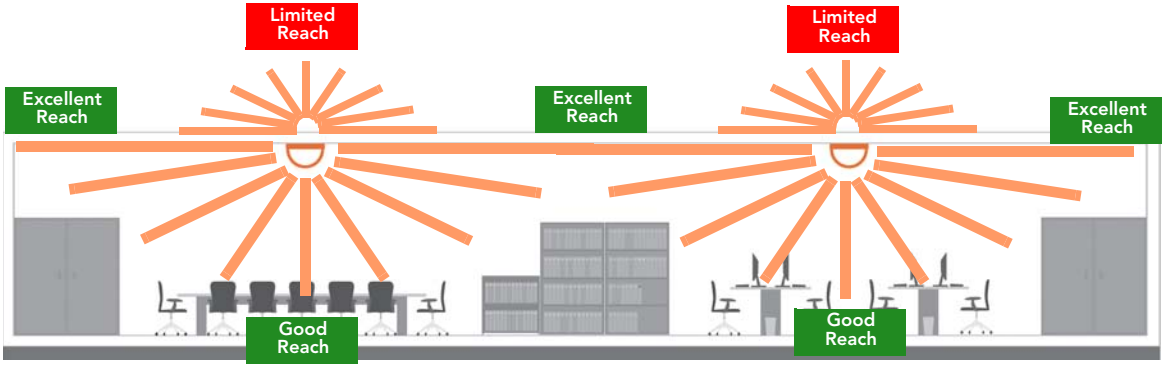


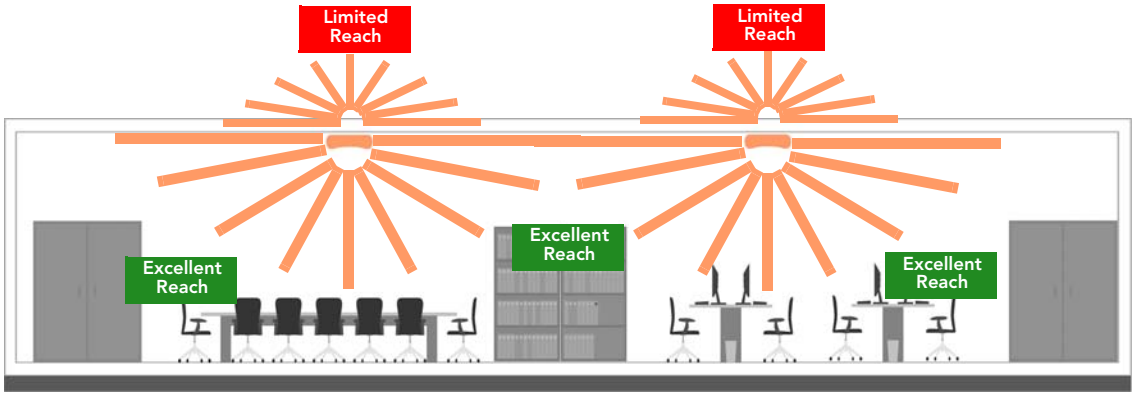
Figure 13. Recommended orientation for maximum mesh coverage



ZoneFlex 7341, 7343 and 7363 Orientation

ZoneFlex 7341, 7343 and 7363 have a more rounded coverage area and less horizontal range (when mounted horizontally) compared to the ZoneFlex 2942, 7942 and 7962 APs.

Figure 14. ZoneFlex 7341/7343/7363 recommended ceiling mounting orientation



When wall mounted, ZoneFlex 7341, 7343 and 7363 should be staggered to maximize coverage.

Figure 15. ZoneFlex 7341/7343/7363 recommended wall mounting orientation

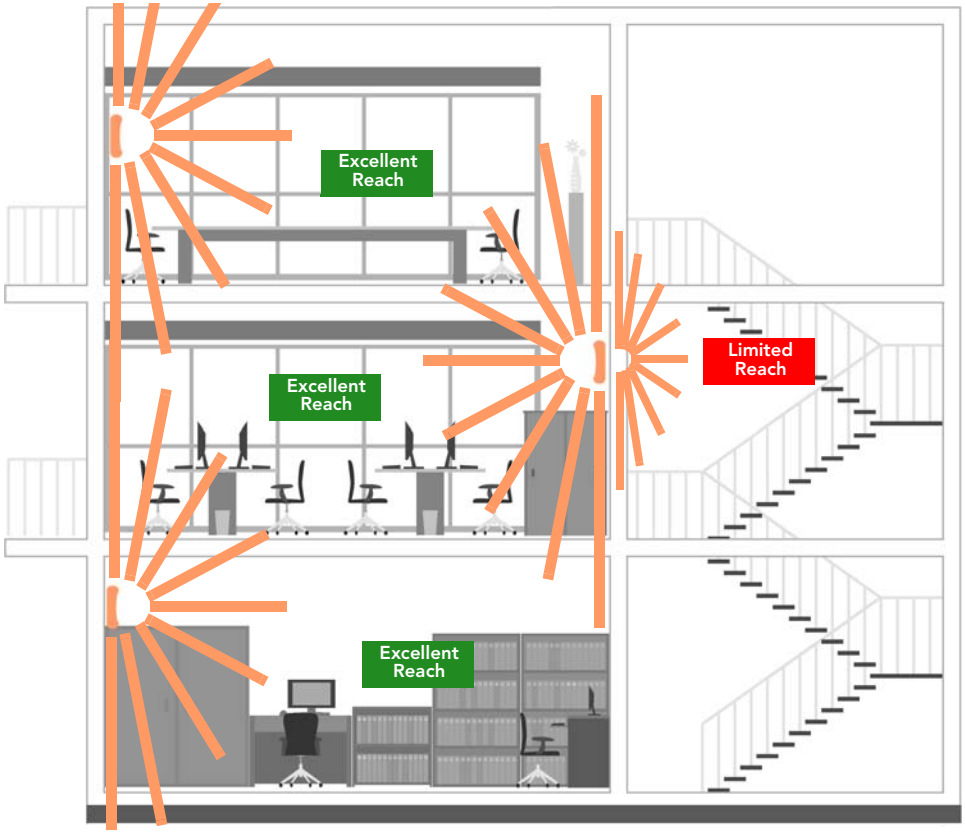
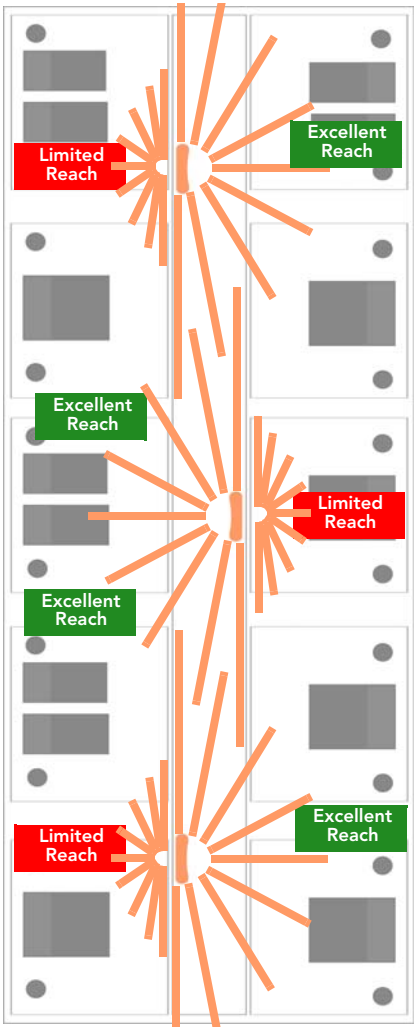


Figure 16. ZoneFlex 7341/7343/7363 wall mounting in a corridor (top view)



Step 1: Preconfigure the Access Point

The procedure for completing the Access Point's essential configuration depends on whether you want it to be managed by either ZoneDirector or FlexMaster or to operate as a standalone Access Point. Refer to the section that is relevant to your deployment:

- Configuring for Management by ZoneDirector
- Configuring for Standalone Operation or for Management by FlexMaster

Configuring for Management by ZoneDirector

If ZoneDirector is installed on the network, you do not need to preconfigure the Access Point for management by ZoneDirector. Simply connect the Access Point to same Layer 2 subnet as ZoneDirector, and when the Access Point starts up, it will discover and register with ZoneDirector automatically.

NOTE: In addition to using Layer 2 auto discovery to enable the Access Point to register with ZoneDirector, you can also use DHCP Option 43 or DNS. For more information, refer to the *ZoneDirector User Guide*.

CAUTION: If you use this method, make sure that you do not change the IP address of ZoneDirector after the AP discovers and registers with it. If you change the ZoneDirector IP address, the AP will no longer be able to communicate with it and will be unable to rediscover it.

CAUTION: If you configure an AP for management by ZoneDirector and later decide that you want it to be a standalone AP, you will need to factory reset the AP.

Before starting this procedure, check the label on the back panel of the Access Point, and write down the MAC address of the Access Point. You will need the MAC address to identify the Access Point on the ZoneDirector Web interface.

What You Will Need

Before starting with the configuration task, make sure that you have the following requirements ready:

- A computer from which you can access the ZoneDirector Web interface
- A Web browser such as Google Chrome, Mozilla Firefox 2.0 (or later) or Microsoft Internet Explorer 6.0 (or later) installed on the administrative computer
- One Cat5e foil screened twisted pair (FTP) solid Ethernet cable
- Your *ZoneFlex Access Point* and its power adapter (or a PoE injector/PoE switch to supply Power Over Ethernet to the Access Point)

1. Connect the Access Point to a Power Source

1. Connect the power jack to the power connector on the rear panel of your ZoneFlex Access Point.
2. Connect the power adapter to a power source.
3. Verify that the power LED on the Access Point is green.

You have completed connecting the Access Point to a power source.

NOTE: If using PoE, you do not need to connect a power adapter to the AP. Simply provide PoE power to the to the port labeled "10/100/1000 PoE" and connect the PoE injector/switch to the same subnet as ZoneDirector.

NOTE: If using PoE and Gigabit Ethernet, ensure that you use Cat5e or better Ethernet cables.

2. Connect the Access Point to the Same Subnet as ZoneDirector

1. Connect one end of an Ethernet cable to a LAN (RJ-45) port on the rear panel of the Access Point.
2. Connect the other end of the Ethernet cable to the same Layer 2 subnet as ZoneDirector. The same Layer 2 subnet means that there should not be any router between the Access Point and ZoneDirector.
3. Log into the ZoneDirector Web interface, and then go to the **Monitor** > **Access Points** page.
4. Look for the MAC address of the Access Point, and then check its **Status** column.
   - If automatic approval is enabled, the Status column should show **Connected**.
   - If automatic approval is disabled, click the **Allow** ✔ link that is on the same row as the Access Point's MAC address. This allows the Access Point to register with ZoneDirector.

When the Status column shows **Connected**, this indicates that the Access Point has successfully registered with ZoneDirector and that it can now be moved to its destination Layer 2 or Layer 3 network.

3. Disconnect the Access Point from the Power Source

1. Disconnect the Access Point from the power source.
2. Verify that the power LED on the rear panel of the Access Point is off.
3. Continue to "Connect the Access Point to the Network" on page 37.

Configuring for Standalone Operation or for Management by FlexMaster

This section describes the steps you need to complete to set up the AP in standalone mode or to be managed by Ruckus Wireless FlexMaster server, if you have one installed on the network.

What You Will Need

Before starting with the configuration task, make sure that you have the following requirements ready:

- An administrative computer (notebook computer) running Microsoft Windows (2000/XP/Vista/7)
- A Web browser such as Google Chrome, Mozilla Firefox 2.0 (or later) or Microsoft Internet Explorer 6.0 (or later) installed on the administrative computer
- One Cat5e foil screened twisted pair (FTP) solid Ethernet cable

1. Prepare the Administrative Computer

NOTE: The following procedure is applicable if the administrative computer is running Windows XP or Windows 7. If you are using a different operating system, refer to the documentation that was shipped with your operating system for information on how to modify the computer's IP address settings.

1. On your Windows XP or Windows 7 computer, open the **Network Connections** (or **Network and Dial-up Connections**) control panel according to how the Start menu is set up:
   - On Windows XP, click **Start** > **Control Panel** > **Network Connections.**
   - On Windows 7, click **Start** > **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**.
2. When the Network Connections window appears, right-click the icon for Local Area Connection, and then click **Properties**.

NOTE: Make sure that you configure the Local Area Connection properties, not the Wireless Network Connection properties.

3. When the **Local Area Connection Properties** dialog box appears, select **Internet Protocol (TCP/IP)** (**TCP/IPv4** in Windows 7) from the scrolling list, and then click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box appears.
4. Write down all of the currently active network settings. You will need this information later when you restore your computer to its current network configuration.

5. Click **Use the following IP address**, and then configure the IP address settings with the values listed in Table 14. For a sample configuration, refer to Figure 17.

Table 14. Configure your computer's IP address settings

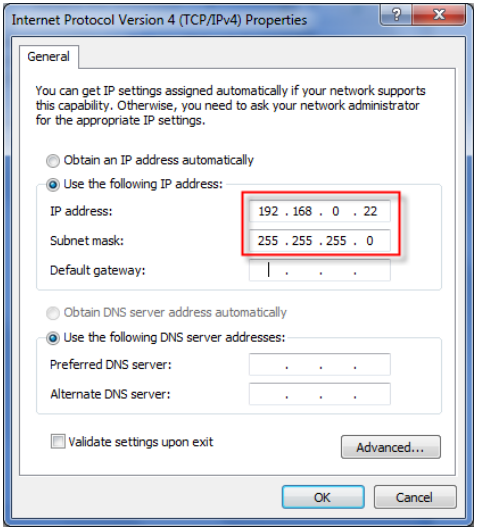
IP address	`192.168.0.22` (or any address in the 192.168.0.x network—with the exception of `192.168.0.1`, which is the default IP address assigned to the Access Point)
Subnet mask	`255.255.255.0`

You can leave the **Default Gateway** and **DNS server** fields blank.

6. Click **OK** to save your changes and close the TCP/IP Properties dialog box.
7. Click **OK** again to close the Local Area Connection Properties dialog box.

Windows saves the IP address settings that you have configured.

Figure 17. Sample configuration in the Internet Protocol (TCP/IP) Properties dialog box


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 22
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

2. Connect the Access Point to the Administrative Computer

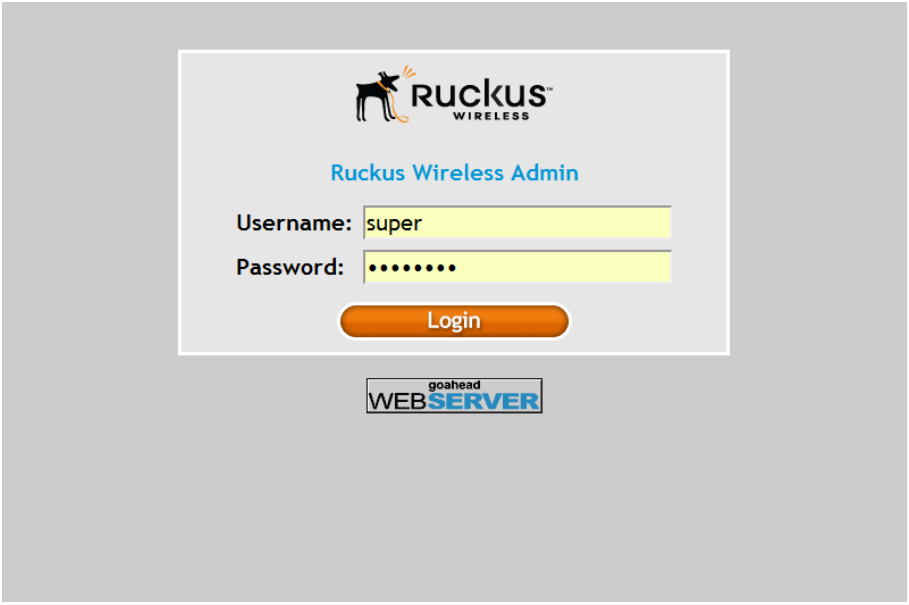
1. Connect one end of an Ethernet cable to an Ethernet port on the Access Point, and then connect the other end to the administrative computer's Ethernet port.
2. Provide power to the AP using either an AC adapter or a PoE injector or switch, as described in "1. Connect the Access Point to a Power Source" above.

3. Log Into the Access Point's Web Interface

1. On the administrative computer, open a Web browser window.
2. In the address or location bar, type the following address:

   `https://192.168.0.1`
3. Press `<Enter>` on the keyboard to connect to the Access Point's Web interface. A security alert message appears.
4. Click **Yes** or **OK** (depending on the browser) to continue. The Access Point's login page appears.

Figure 18. The ZoneFlex Access Point login page



5. In **User name**, type `super`.
6. In **Password**, type `sp-admin`.
7. Click **Log In**. The Web interface appears, displaying the *Status* > *Device* page.
8. Continue to "4. Configure the Wireless Settings" below.

4. Configure the Wireless Settings

To complete this step, you will need to configure the settings on the **Common** tab and at least one **Wireless #** tab. These are the essential wireless settings that will enable wireless devices on the network to associate with the Access Point.

For your reference, the default wireless settings on the Access Point are listed in Table 15.

Table 15. Default wireless settings

Setting	Default Value
SSID (network name)	Wireless 1 to Wireless 8 (2.4 Ghz Radio) Wireless 9 to Wireless 16 (5 GHz Radio - only available on dual radio APs)
Encryption (security)	Disabled on all WLANs
Default management IP address	`192.168.0.1`

Configure Common Wireless Settings

1. On the left menu of the Web interface, click **Configuration** > **Wireless (Radio 2.4G** or **Radio 5G** on dual band APs**)**. The *Configuration > Common* page appears.

NOTE: For dual band APs (ZoneFlex 7962 and 7363), the two radios (2.4GHz and 5GHz) need to be configured separately on the Web interface. To configure the common wireless settings, click **Configuration** > **Radio 2.4G** or **Radio 5G**. The rest of the configuration procedures are the same as for other models.

2. Verify that the common wireless settings are configured as listed in Table 16.

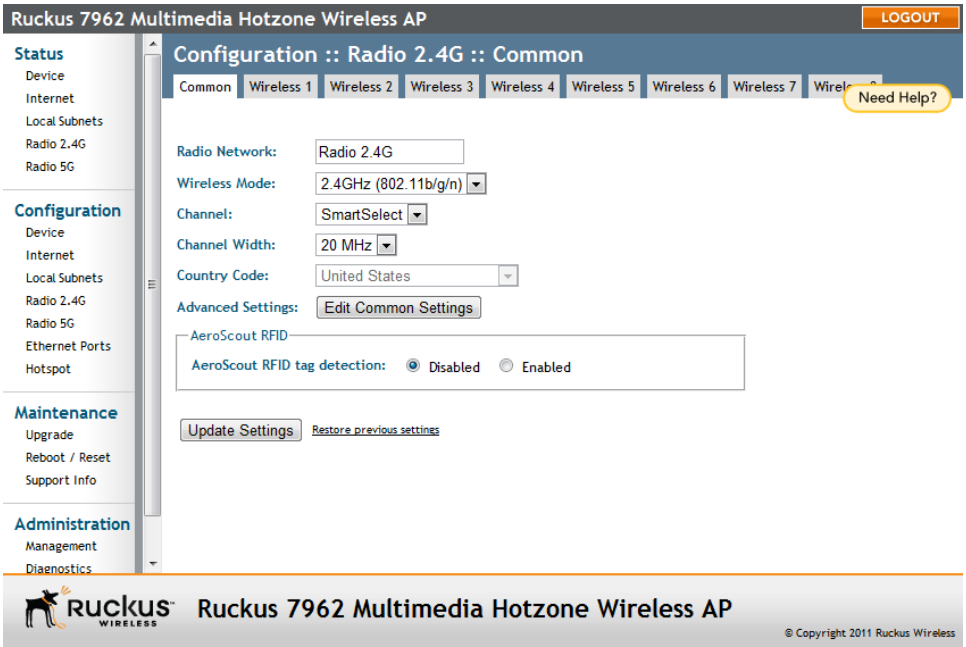
Table 16. Common wireless configuration

Setting	Recommended Value
Channel	SmartSelect
Country Code	• If you purchased the Access Point in the United States, this value is fixed to **United States** at the factory and is not user configurable. • If you purchased the Access Point outside the United States, verify that the value is set to your country or region. Selecting the correct country code ensures that the Access Point uses only the radio channels allowed in your country or region. *Note for dual band AP users: The two radios on dual band APs are always configured with the same country code setting. If you change the country code for Radio 1, for example, the same change will be applied automatically to Radio 2.*

3. If you made any changes to the **Common** tab, click **Update Settings**.

4. Continue to "Configure Wireless # Settings" below.

Figure 19. The Configuration > Wireless > Common tab



Configure Wireless # Settings

1. Click one of the **Wireless #** tabs.
2. In **Wireless Availability**, click **Enabled**.
3. In **Broadcast SSID**, click **Enabled**.
4. Clear the **SSID** box, and then type a unique and descriptive name that you want to call this wireless network.

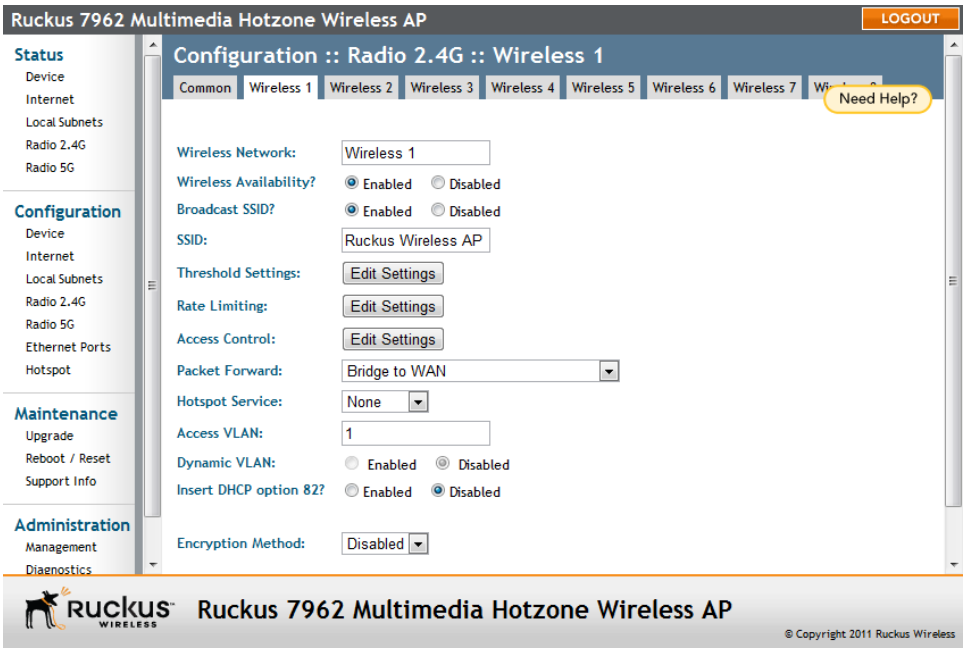
   For example, you can type `Ruckus Wireless AP`. This SSID is the name that will help users identify this wireless network in their wireless network connection application.

NOTE: You may also configure other wireless settings on this and other **Wireless #** tabs (in addition to the settings described above), although it is not necessary for completing the Access Point installation.

5. Click **Update Settings**.

You have completed configuring the basic wireless settings of the Access Point.

Figure 20. The Configuration > Wireless > Wireless 1 tab



(Optional) Set the FlexMaster Server Address

If you have a FlexMaster server installed on the network and you intend to use FlexMaster to manage the Access Point, you can set the FlexMaster server address at this point. Before starting this procedure, make sure you obtain the correct FlexMaster server URL.

NOTE: In addition to setting the FlexMaster server URL manually on the Access Point, you can also use DHCP Option 43 or DNS to point the Access Point to the FlexMaster server. For more information, refer to the *FlexMaster User Guide*.

1. On the menu, click **Administration** > **Management**.
2. Scroll down the page to the **TR069 / SNMP Management Choice** section.
3. Verify that the **Auto** option is selected.
4. In **FlexMaster Server URL**, type the URL of the FlexMaster server on the network. You can use either `http` or `https` to connect to the URL and include either the host name or IP address of the FlexMaster server in the URL. The following are examples of valid FlexMaster server URLs:

   `http://flexmaster/intune/server`

   `https://flexmaster/intune/server`

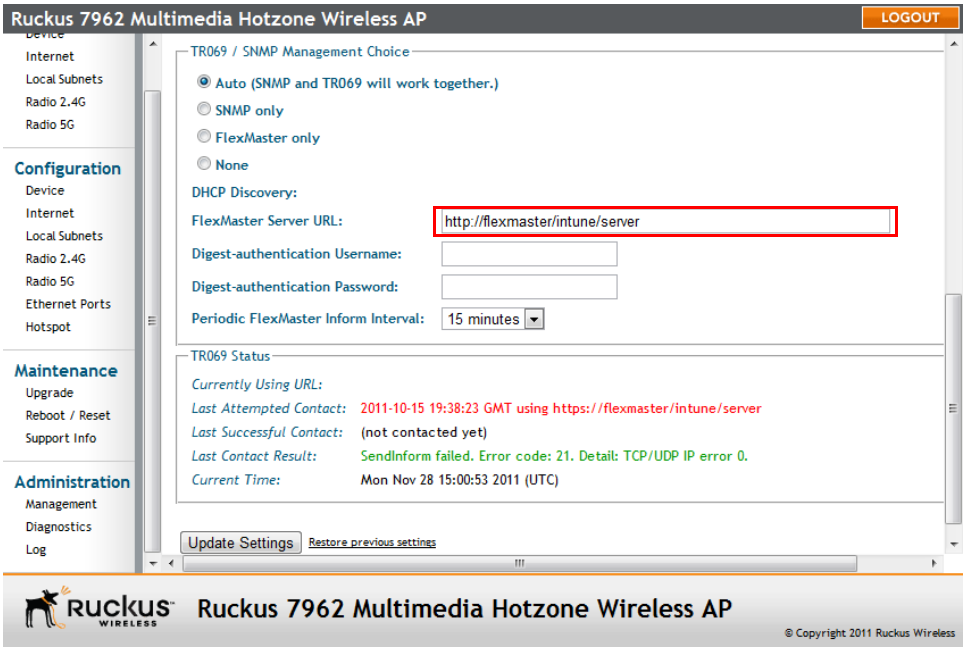
   `http://192.168.20.1/intune/server`

```
https://192.168.20.1/intune/server
```

5. Click **Update Settings** to save your changes.

You have completed setting the FlexMaster server address on the Access Point.

Figure 21. Type the FlexMaster server URL



NOTE: Instructions on how to verify that the Access Point and FlexMaster can communicate with each other are provided in "Check the TR069 Status (FlexMaster Management Only)" on page 38.

5. Disconnect the Access Point from the Administrative Computer

1. Disconnect the Access Point from the power source.
2. Verify that the power LED on the Access Point is off.
3. Disconnect the Ethernet cable from the administrative computer's Ethernet port.

6. Restore the Administrative Computer's Network Settings

1. On your Admin computer, open the **Network Connections** (or **Network and Dial-up Connections**) control panel according to how the Start menu is set up:

- On Windows 7, click **Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**.
- On Windows XP, click **Start** > **Control Panel** > **Network Connections.**

2. When the Network Connections window appears, right-click the icon for **Local Area Connection**, and then click **Properties**.
3. When the **Local Area Connection Properties** dialog box appears, select **Internet Protocol (TCP/IP)** (**TCP/IPv4** in Windows 7) from the list, and then click **Properties**. The **TCP/IP Properties** dialog box appears.
4. Restore the computer's network settings by typing the original IP address settings in the **TCP/IP Properties** dialog box.
5. On the **TCP/IP Properties** dialog box, click **OK** to close it.
6. Click **OK** again to close the **Local Area Connection Properties** dialog box.

You are now ready to connect the Access Point to your network.

Step 2: Verify Access Point Operation

Before deploying the Access Point in your environment, Ruckus Wireless strongly recommends that you verify that the Access Point is operating correctly. To do this, you will need to connect the Access Point to your live network temporarily and make sure that the network connection works and that wireless clients are able to associate with the Access Point and connect to your network and the Internet.

NOTE: The network and power connections that you will be making in this step are temporary.

Connect the Access Point to the Network

1. Connect the Ethernet cable from a LAN (RJ-45) port on the Access Point to your network's router or switch.
2. Reconnect the Access Point to a power source.

You have completed connecting the Access Point to your live network. Perform the tasks described in the following sections to verify that the Access Point is operating normally.

Associate a Wireless Client with the Access Point

1. On the administrative computer, verify that the wireless interface is enabled. On Windows XP, click **All Programs** > **Connect To** > **Wireless Network Connection** to enable the wireless interface. (Other operating systems are similar).
2. Connect your admin computer to the wireless network:

- *Windows XP*: In the system tray, right-click the (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.
- *Windows 7*: Left click the icon.

3. In the list of available wireless networks, click the network with the same SSID as you configured in "Configure Wireless # Settings" on page 34. For example, if you set the SSID to `Ruckus Wireless AP`, click the wireless network named **Ruckus Wireless AP**.
4. Click **Connect**.

Your wireless client connects to the wireless network. After the wireless client connects to the wireless network successfully, the wireless client icon in the system tray changes to (on Windows XP) or (on Windows 7).

Check the LEDs

Perform a spot-check using the LEDs to verify that the Access Point is operating normally. Refer to the following sections for information on how to check the LEDs on each ZoneFlex AP model.

Single Radio APs (ZoneFlex 2942/7942/7341/7343)

If the single radio Access Point is operating normally and your wireless client was able to associate with it:

- The **WLAN** LED is green.
- If you do not have Ruckus Wireless ZoneDirector on the network, the **DIR** LED is off. This indicates that the Access Point is operating in standalone mode. If there is a ZoneDirector device on the network, the **DIR** LED is green.

Dual Radio APs (ZoneFlex 7363 and 7962)

If the dual radio Access Point is operating normally and your wireless client was able to associate with it:

- The **2.4G** or **5G** LED is green.
- If you do not have Ruckus Wireless ZoneDirector on the network, the **DIR** LED is off. This indicates that the Access Point is operating in standalone mode. If there is a ZoneDirector device on the network, the **DIR** LED is green.

Check the TR069 Status (FlexMaster Management Only)

If you configured the Access Point to report to a FlexMaster server on the network, make sure you verify that it can successfully communicate with the FlexMaster server. You can do this by checking the TR069 status on the Access Point's Web interface.

1. Log in to the Access Point's Web interface.

2. Go to the **Administration** > **Management** page.
3. Scroll down to the **TR069 Status** section.
4. Check the value for **Last successful contact**. If it shows a date in green, this indicates that the Access Point was able to successfully communicate with FlexMaster.

Disconnect the Access Point from the Network

1. Disconnect the Access Point from the power source.
2. Disconnect the Ethernet cable that runs to the Access Point's RJ45 port from your network's router or switch.

You are now ready to deploy the Access Point to its permanent mounting location.

Step 3: Deploy the Access Point

In this step, you will place the Access Point in a suitable location on the network and connect it to a power source and to your network environment.

1. Choose a Location for the Access Point

You can install the Access Point on a flat surface (for example, on a desktop or tabletop) or mount it on a wall or ceiling. When choosing a location for the Access Point, ensure that the location:

- Allows easy viewing of the LEDs and access to the connectors, if necessary.
- Is centrally located to the wireless clients that will be connecting to the Access Point. A suitable location might be on top of a cabinet or similar furniture to optimize wireless connections to clients in both horizontal and vertical directions, allowing wider coverage.

When positioning your Access Point, ensure that:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- There are no thick walls or metal shielding between the Access Point and the wireless stations.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted.

Review the recommendations in "Determine the Optimal Mounting Location and Orientation" on page 23 for help in choosing a suitable location for the Access Point.

2. Connect the Access Point to a Power Source and the Network

Once you have placed the Access Point at its installation location, you are ready to connect it to a power source and the network.

NOTE: If your ZoneFlex model supports PoE, you can also supply power to the AP from a PoE switch or injector. For information on how to make the PoE connections, refer to the documentation that was shipped with the PoE switch or injector.

CAUTION: If you will be using PoE, you must use a Cat-5e or better Ethernet cable for the PoE connection.

1. Connect the power jack to the power connector on the rear panel of your ZoneFlex Access Point.

2. Connect the power adapter to a power source.
3. Obtain an Ethernet cable that is long enough to connect the Access Point to your network's router, switch, or hub.
4. Connect one end to a LAN port on the AP, and then connect the other end to your network's router, switch, or hub.
5. Verify that the power LED on the Access Point is green.

Congratulations! You have completed setting up the Access Point on your network. To learn how to configure and manage the Access Point, continue reading the next chapters.

Troubleshooting Installation

If the startup sequence does not work, verify that the network name (SSID) and security settings (if you enabled them) on the AP match the settings on your wireless device.

- Disconnect the AP from the power source, wait 5 seconds, reconnect it, and then wait 60 seconds before attempting a reconnection.
- Disconnect and reconnect the AP and the PC.
- Replace the Ethernet cable with a new one if the relevant LAN port LED is not illuminated. (LEDs in each port light up during a successful connection.)

If all else fails, you can reset the AP to its factory defaults (and start over).

1. Insert a straightened-out paper clip into the reset button hole.
2. Press and hold the **Reset** button for at least eight (8) seconds.

You can now reconnect your computer directly to the AP (as described in "2. Connect the Access Point to the Administrative Computer" on page 31), and then start over with installation, using the default network settings.

3

Navigating the Web Interface

In This Chapter

Logging Into the ZoneFlex Web Interface 43
Navigating the Web Interface 44

Logging Into the ZoneFlex Web Interface

If you need to manage your AP, you do it with the features of the ZoneFlex Web interface (which you already used to set up the AP for use).

If your ZoneFlex network will be managed by a Ruckus Wireless ZoneDirector, you can manage APs through ZoneDirector rather than logging into each AP's Web interface individually.

NOTE: The following procedure assumes that you know the static IP address of the AP (now in use), or you have some means of determining the dynamic IP address in use by the AP. The PC you use for AP administration should be on the management VLAN, if VLANs are used in your network.

To log into the Web interface

1. On the PC, open a Web browser window.
2. In the address or location bar, type the IP address of the AP. Default IP address for standalone ZoneFlex APs:

   `192.168.0.1`
3. Press <Enter> to connect to the Web interface.
4. If a Windows security alert dialog box appears, click **OK**/**Yes** to proceed. The Ruckus Wireless Admin login page appears.
5. In **Username**, type `super`.
6. In **Password**, type `sp-admin`.
7. Click **Login**.

The ZoneFlex Access Point Web interface appears.

Navigating the Web Interface

You manage the Access Point through a Web browser-based interface that you can access from any networked computer. Table 17 lists the Web interface features that are identified in Figure 22.

Figure 22. Elements of the ZoneFlex AP Web Interface

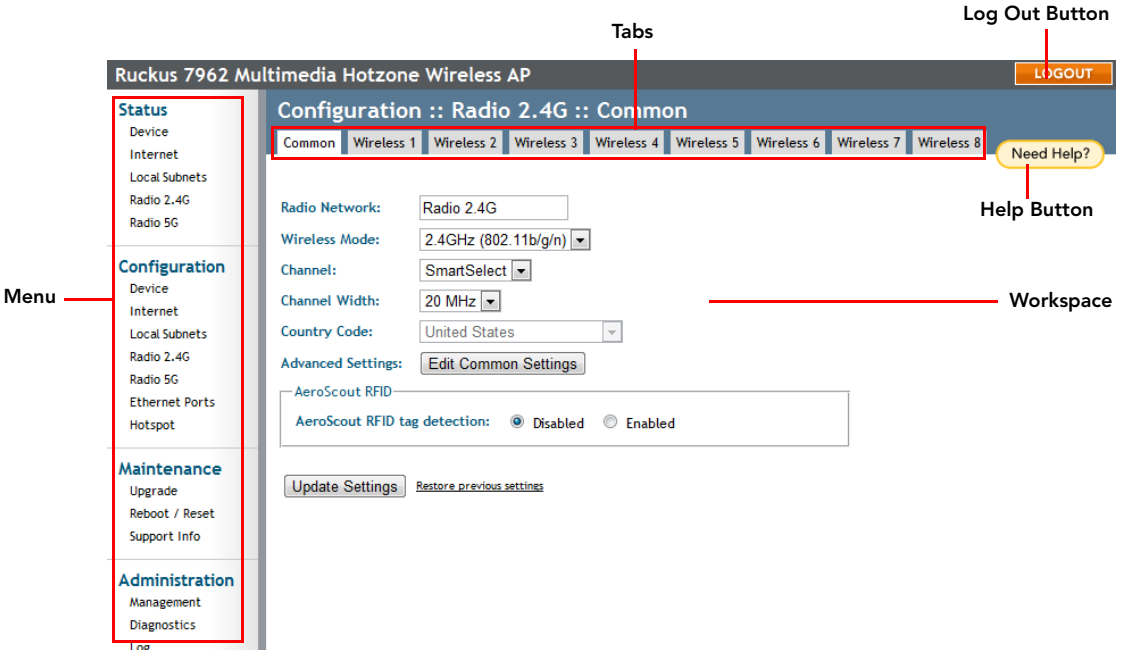


Table 17. ZoneFlex AP Web interface elements

Element	Description
Menu	Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.
Tabs	Contains additional options for the configuration page. For example, the **Configuration** > **Wireless** page includes one tab for common wireless configuration and eight tabs for each of the available WLANs.
Workspace	This large area displays features, options and indicators relevant to your menu bar choices.
Logout Button	Click this button to log out of the AP.

Table 17. ZoneFlex AP Web interface elements

Element	Description
Help Button	Click this button to open a help window with information related specifically to the options currently displayed in the workspace.

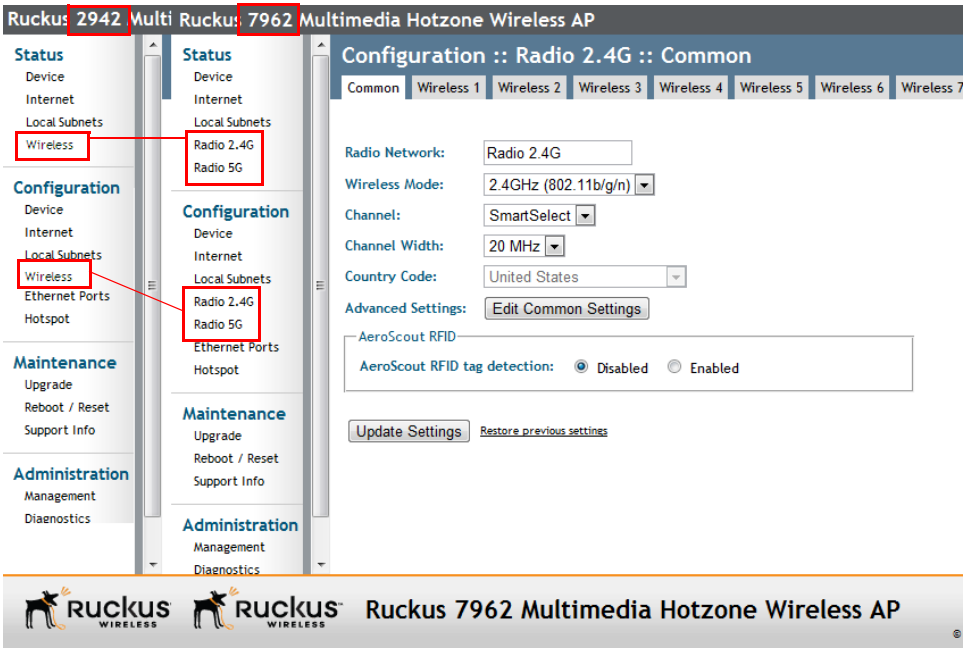
If You Are Using a Dual Band ZoneFlex Access Point

If your ZoneFlex AP model is 7363/7962, note that elements on the Web interface menu are slightly different from the other (single band) ZoneFlex AP models.

Dual band ZoneFlex APs have one 2.4GHz radio (for 802.11b/g/n clients) and one 5GHz radio (for 802.11a/n clients). The wireless settings for these two radios need to be configured separately, which is why the dual band AP Web interface has the **Radio 2.4G** and **Radio 5G** menu items, instead of a single **Wireless** menu item in other models.

Figure 23 highlights the differences between the ZoneFlex 7962 and ZoneFlex 2942 menus.

Figure 23. Menu items are slightly different in dual band APs (left) and other ZoneFlex AP models (right)



4

Configuring the Access Point

In This Chapter

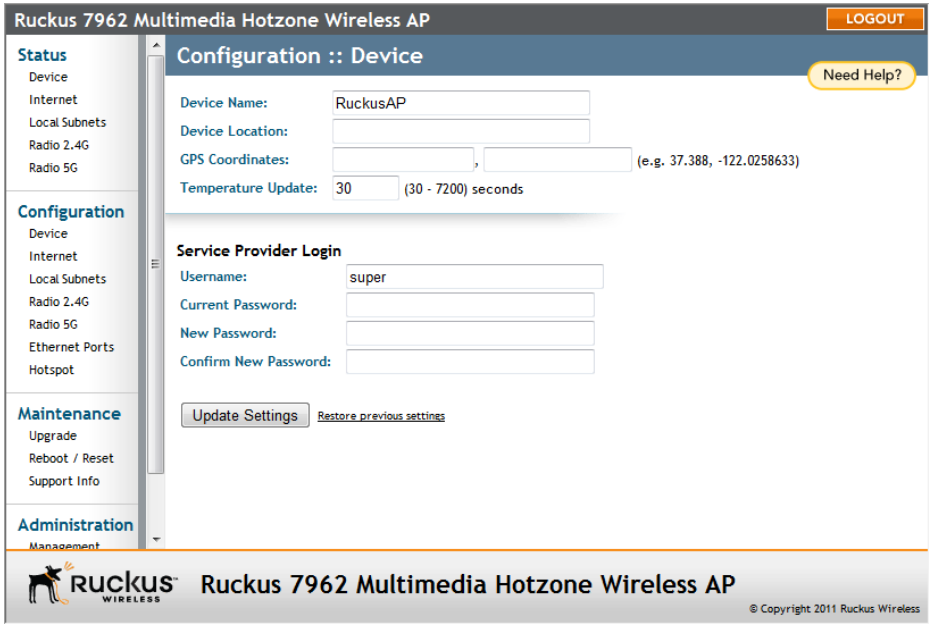
Configuring Device Settings 48
Configuring Internet Settings 49
Configuring Local Subnets 55
Configuring Wireless Settings 56
Configuring Ethernet Ports 75
Configuring Hotspot Service 80

This chapter provides instructions for configuring ZoneFlex Access Points in a stand-alone environment. If you will be managing your ZoneFlex network using ZoneDirector refer to the ZoneDirector User Manual, available in PDF format from the Ruckus website, at http://support.ruckuswireless.com/documents.

Configuring Device Settings

Device settings refer to the device name, temperature update, location and service provider login settings. (Temperature update is only available on certain ZoneFlex models.)

Figure 24. The Configuration > Device page



To configure the device settings

1. Go to **Configuration** > **Device**. The Configuration > Device page appears.
2. In **Device Name**, type a new name for the device or leave as is to accept the default device name (`RuckusAP`). The device name identifies the Access Point among other devices on the network.
3. Optionally, enter **Device Location** and **GPS Coordinates** to keep track of the physical location of the AP. In **Temperature Update** (specific models only), enter the interval (in seconds) to record the internal temperature of the device.
4. Under **Service Provider Login**, change the login information as required:
   - **Username**: Type the name that you want to use for logging into the Web interface. The default user name is `super`.
   - **Password**: Type the new password that you want to use. The default password is `sp-admin`. The password must consist of six to 32 alphanumeric characters only.
   - **Confirm New Password**: Retype the new password to confirm.

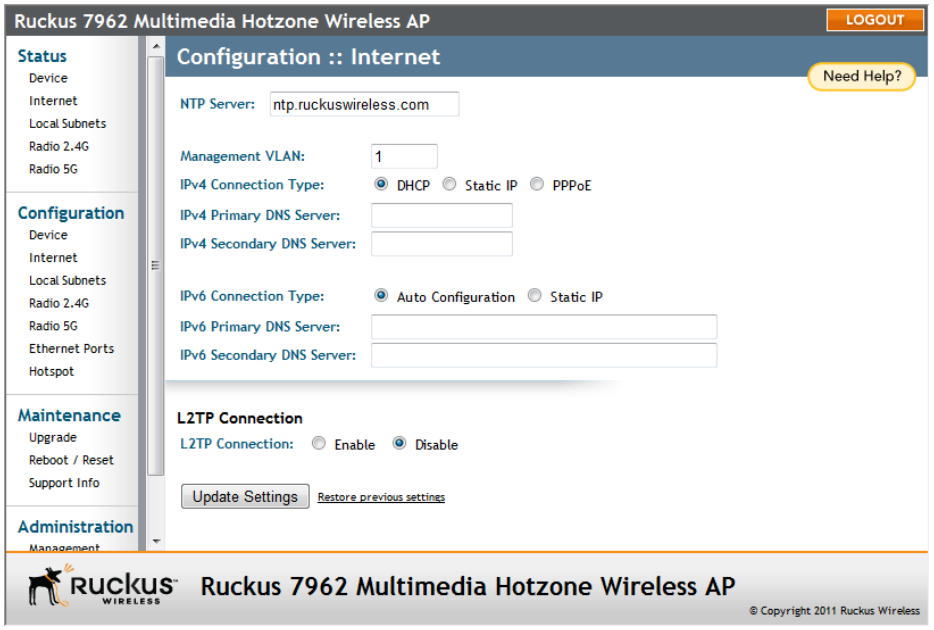
5. Click **Update Settings** to save and apply your changes.

Configuring Internet Settings

Internet settings define how the Access Point connects to your local area network and to the Internet. This section describes how to view and configure the Access Point's Internet settings. Topics discussed include:

- VLAN Settings Overview
- Configuring NTP Server and Management VLAN
- Default IP Addressing Behavior
- Obtaining and Assigning an IP Address
- Configuring L2TP Connection Settings

Figure 25. The Configuration > Internet page



VLAN Settings Overview

A Ruckus Wireless access point is essentially a network switch with the capability to service Wi-Fi connections. As such, like many advanced switches, Ruckus APs conform to the IEEE 802.1Q standard -- the standard that defines virtual LANs. In an 802.1Q switch, the concept of VLANs is always present. If a packet arrives without an 802.1Q header, it is assigned to the "native VLAN" or "untag VLAN."

Each of the AP's wireless interfaces can be assigned a single VLAN. When a packet enters the AP through its wireless interface, the packet is assigned to the Access VLAN configured on the Configuration > Wireless page (by default, 1).

AP Ethernet ports however, can be configured to pass all VLAN traffic (Trunk Ports) or multiple specific VLANs (General ports).

The VLAN displayed in the Web interface shows the AP's view of the VLAN environment; when a packet arrives at an AP's Ethernet port, the port's VLAN configuration helps determine if the packet is accepted or not (VLAN membership), and assign a default VLAN (untagged VLAN) if the packet contains no 802.1Q header.

In general, if your network has VLANs deployed already, you should apply VLAN configuration to Ruckus APs so that the configuration across the network is consistent.

Configuring NTP Server and Management VLAN

NTP Server

A Network Time Protocol (NTP) Server should be configured to ensure that the Access Point maintains the correct time. The default Ruckus Wireless NTP Server (ntp.ruckuswireless.com) can be used if you do not have an NTP server on your network.

If you want the AP to contact a different NTP server, you can do so by going to **Configuration > Internet** and entering the host name in **NTP Server** at the top of the page.

Management VLAN

CAUTION: Changing the Management VLAN will cause you to be immediately disconnected from the Web interface if the computer you are using is not on the same VLAN. Do not change the Management VLAN unless your admin PC is on the same VLAN, or you will be disconnected and unable to connect again without factory resetting the AP.

If you want to place this AP's management traffic into a management VLAN, enter the VLAN ID in the **Management VLAN** field and click **Update Settings**.

Default IP Addressing Behavior

By default, the Access Point is configured to automatically obtain an IPv4 address from a DHCP server on the network. If the Access Point does not detect a DHCP server, it automatically assigns itself the static IP address `192.168.0.1` to make it easier for you to preconfigure and deploy it on your network.

For IPv6, the Auto Configuration setting serves the same purpose as DHCP. The default static IPv6 address is `fc00::1`.

Obtaining and Assigning an IP Address

There are three methods of assigning IP addresses to the Access Point:

- DHCP / Auto Configuration
- Static IP
- PPPoE

DHCP / Auto Configuration

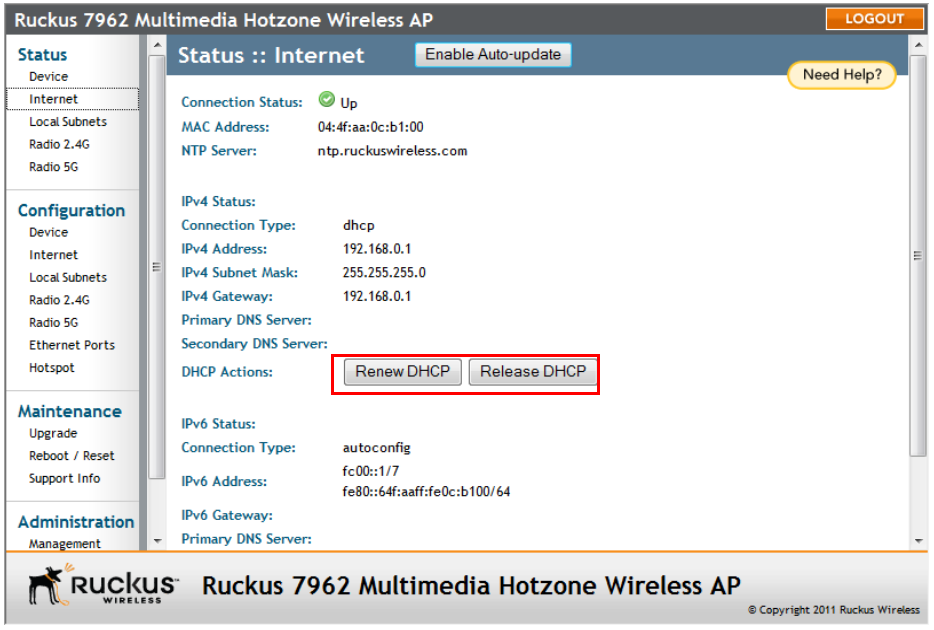
If you leave the Access Point at its default configuration, it will attempt to obtain an IPv4 address from a DHCP server on the network.

In an IPv6 network environment, the AP will attempt to obtain an IPv6 address from an IPv6 Auto Configuration server.

Renewing and Releasing DHCP

This task should be performed only if you have access to the DHCP server or have some way to determine what IP address has been assigned to the AP. It serves as a troubleshooting technique when IP addresses to one or more networked devices prove to be unusable or in conflict with others, or when the AP loses its DHCP-assigned IP address for some reason.

Figure 26. Renew or Release DHCP



To renew or release the DHCP server-assigned IP address

1. Go to **Status** > **Internet**.

2. Review the current settings.
3. If the current **Connection Type** is **DHCP**, you will be able to see the currently-assigned IP address and subnet mask listed below.
   - To force the AP to release its DHCP-assigned IP address, click **Release DHCP**. This will disconnect the user from Web interface as the system reverts to its default IP address. Log in to the device using the default IP address (192.168.0.1) and click on **Renew DHCP** to request a new lease from the DHCP server.
   - Click **Renew DHCP** to request a new IP address lease from the DHCP server. *Note: The IP address may or may not change depending on the lease time offered to this device.*
4. Click **Update Settings** to save your settings.

Static IP

There are at least two instances when you would want to configure a static IP address for the Access Point:

- If the current IP address that the Access Point is using consistently conflicts with that of another device on the network.
- If you want to switch from DHCP to static IP addressing, for use in managing or maintaining the Access Point.

Unless you are able to determine the IP address assigned by the DHCP/Auto Configuration server to the Access Point, it may prove helpful for anyone needing administrative access to assign a static IP address.

To assign a static IP address to the AP

1. Go to **Configuration** > **Internet**. The *Configuration > Internet* page appears.
2. You can configure static addresses for IPv4, IPv6 or both. The AP will maintain both sets of IP address settings if both are configured.
3. In *IPv4 Connection Type* or *IPv6 Connection Type*, select **Static IP**.
4. When the *Internet Connection Settings* options appear, you can make changes to the following settings:
   - **Primary DNS Server**: The IP address of the primary Domain Name System (DNS) server.
   - **Secondary DNS Server**: The IP address of the secondary Domain Name System (DNS) server.
   - **IPv4/IPv6 Address**: Enter the static IP address that you want to assign to the AP in either IPv4 (dot-decimal) or IPv6 (colon-separated) format.
   - **Subnet Mask (IPv4)/Prefix Length (IPv6)**: Enter the subnet mask or prefix length for the network.
   - **Gateway**: Enter the gateway IP address of the Internet interface.
5. Click **Update Settings** to save your changes.

PPPoE

Point to Point Protocol over Ethernet (PPPoE) is a Layer 2 protocol which uses the PPP (Point to Point) protocol to connect a client system to a server system over a one to one network link. All traffic for a PPPoE connected client must go through the PPPoE server to reach the client. A PPPoE server can therefore be used to route, NAT, firewall, and perform QoS traffic shaping.

If a PPPoE server is used to distribute Internet access to subscribers, the Access Point can be configured with a PPPoE username and password to authenticate with the PPPoE server.

PPPoE is available only for the IPv4 connection type; PPPoE is not supported in IPv6 environments.

To set the IPv4 connection type to PPPoE

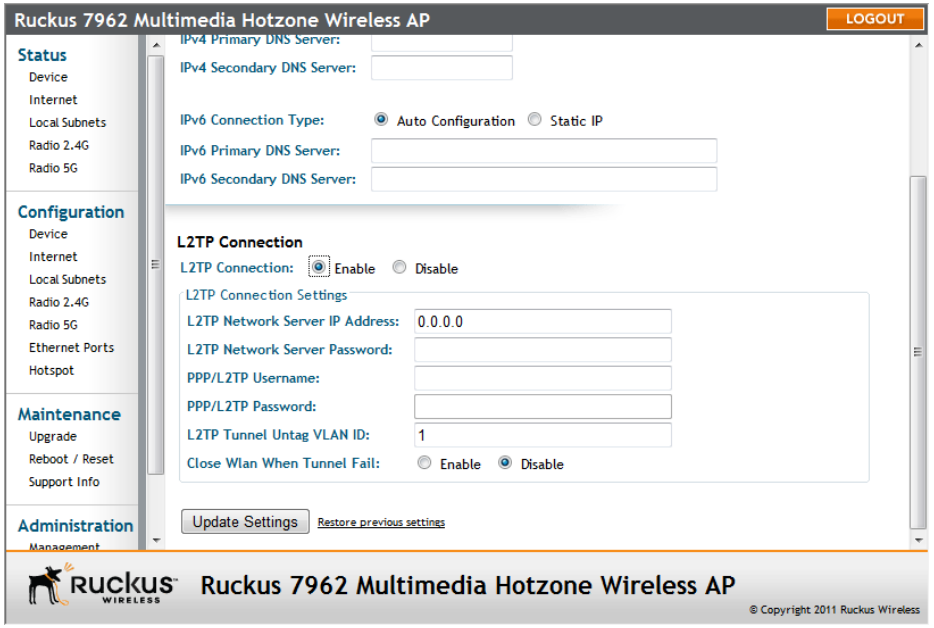
1. Go to **Configuration > Internet**.
2. Under *IPv4 Connection Type*, select **PPPoE**.
3. Enter an **IPv4 Primary DNS Server** address. *Secondary DNS server* is optional.
4. Enter a **PPPoE Username**.
5. Enter a **PPPoE Password**.
6. Retype the password in **PPPoE Password Confirmation**.
7. Click **Update Settings** to save your changes.

Configuring L2TP Connection Settings

You can implement transparent bridging with ZoneFlex through the use of L2TP (Layer 2 Tunneling Protocol) tunneling. By tunneling traffic from a ZoneFlex AP to a centralized data center, access controllers with policy enforcement software can apply rules and services. In a typical WLAN implementation, these rules include a captive portal to authenticate users' credentials.

In the case of L2TP, the ZoneFlex AP functions as a remote bridge. As such, it forwards traffic into PPP sessions over the L2TP tunnel. This implementation ensures that you have complete visibility into MAC addresses of users, as individual Wi-Fi clients are essentially placed (bridged) onto the ISP's core network.

Figure 27. L2TP Connection



To configure L2TP tunneling

1. Go to **Configuration** > **Internet**.
2. Under **L2TP Connection**, click **Enable**.
3. In **L2TP Network Server IP Address**, type the IP address of the L2TP network server (LNS) to which the device will connect.
4. In **L2TP Network Server Password**, type the L2TP server password.
5. If your network requires PPP authentication, configure the following fields under L2TP/PPP Authentication:
   - **Username**: Type your appropriate PPP user name.
   - **Password**: Type the password appropriate to the account.
   - **L2TP Tunnel Untag VLAN ID**: Enter the Untag VLAN ID for the L2TP tunnel.
6. In **Close WLAN When Tunnel Fail**, select **Enable** if you want to disable the WLAN when the tunnel connection is lost. This prevents clients from remaining seemingly connected to the WLAN but without Internet connectivity.
7. Click **Update Settings** to save your settings.

Configuring Local Subnets

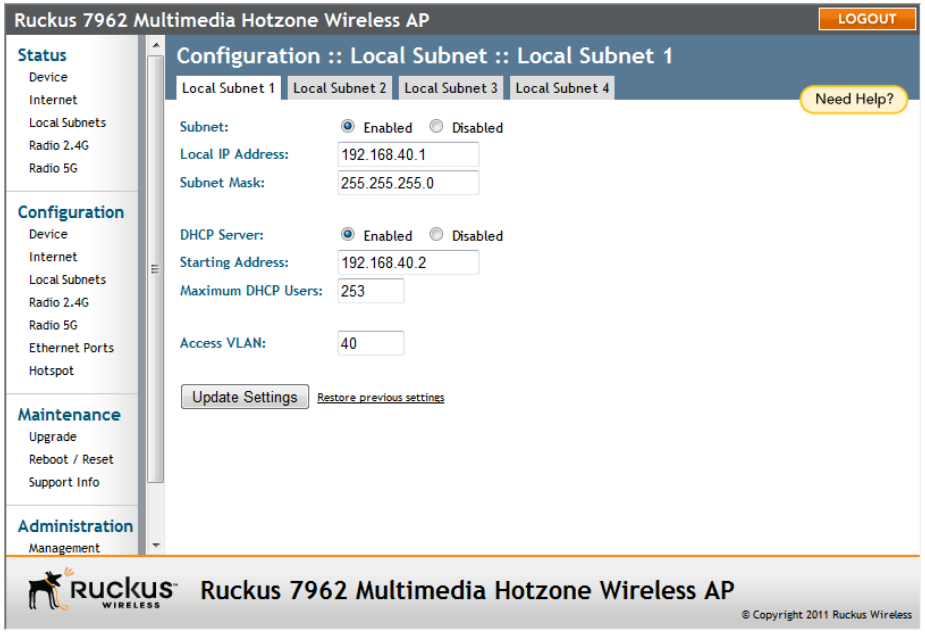
ZoneFlex Access Points can be configured to provide routing/network address translation (NAT) functionality by using the Local Subnets feature. When a Local Subnet is enabled, the standalone AP plays the role of a gateway router with the ability to manage its own subnets, providing DHCP server and DNS cache functions for both wired and wireless clients. These clients can be assigned private IP addresses from a user-defined address pool. Traffic from the client station in private address space appears on the outside as if generated by the AP itself. In this way, the AP performs Layer 3 packet forwarding not only for Hotspot/WISPr usage, but for standard usage as well.

Up to four IP subnets can be configured per AP, each with its own VLAN and address range which cannot conflict with one other.

To configure a local subnet for router mode support

1. Go to **Configuration > Local Subnets**. The four tabs at the top (*Local Subnet 1 - 4*) allow you to configure each of the four subnets independently.
2. Click **Enabled** next to **Subnet**. The local subnet configuration options appear.
3. In **Local IP Address**, enter an IP address for the gateway. The default address for Subnet 1 is `192.168.40.1`. This address can be used to access the AP's Web interface for configuration and monitoring from devices connected to this subnet.
4. In **Subnet Mask**, typically you would want to leave the setting at its default value (`255.255.255.0`) for a Class C subnet with an address pool of up to 254 addresses. An error appears if you enter an invalid IP/netmask combination.
5. In **DHCP Server**, click **Enabled** if you want to enable DHCP for this subnet. Starting Address and Maximum DHCP Users fields appear.
6. In **Starting Address**, enter an address in the same subnet as the Local IP Address (e.g., **`192.168.40.2`**).
7. In **Maximum DHCP Users**, enter the maximum number of clients that can be assigned addresses by DHCP in this subnet (valid values are 1-253 if the default subnet mask is used).
8. In **Access VLAN**, enter a VLAN ID to segment client traffic arriving from this subnet from other network traffic. (Example: if you use the default 192.168.40.1 address range, you would generally want to use "40" as the VLAN for this subnet.)
9. Click **Update Settings** to save your changes. The local subnet is created immediately and can now be applied to WLANs or Ethernet ports from their respective configuration pages.

Figure 28. Configuring local subnets and enabling router mode



Configuring Wireless Settings

This section describes how to configure the wireless settings of the Access Point. There are two types of wireless settings that you need to configure:

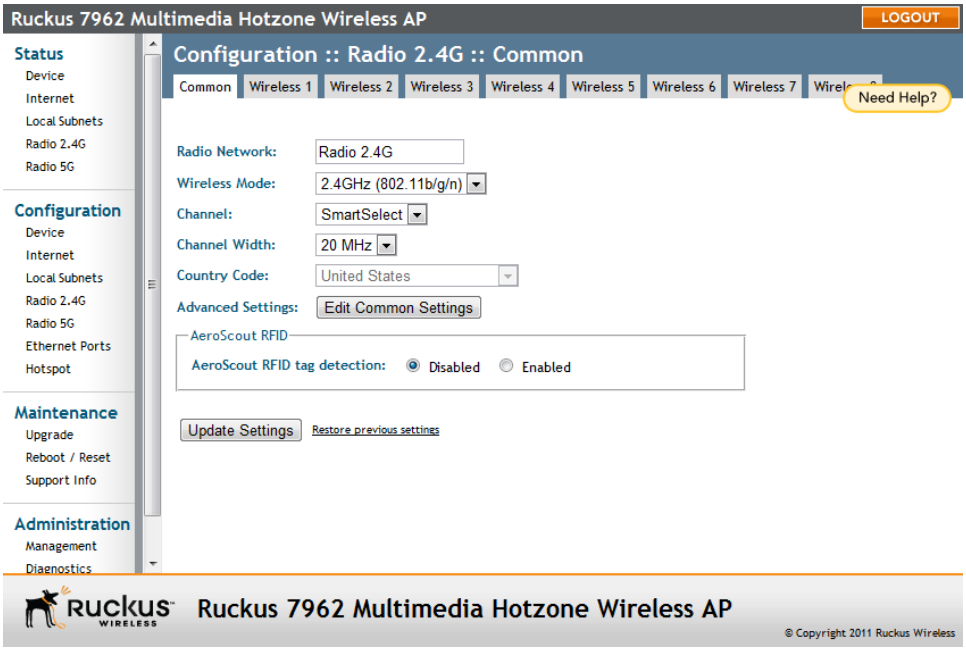
- Configuring Common Wireless Settings: Includes the wireless mode, country code, and advanced wireless settings, such as the wireless transmit power and wireless protection mode. These settings are applied to all WLANs.
- Configuring Wireless # Settings: The Wireless # tabs ("Wireless 1" through "Wireless 8" on the 2.4GHz radio and "Wireless 9" through "Wireless 16" on the 5GHz radio) provide settings for customizing each WLAN individually.

Refer to the sections below for instructions on how to configure each set of wireless settings.

Configuring Common Wireless Settings

Common wireless settings are settings that are applied to all WLANs. On single radio APs, go to **Configuration > Wireless**. On dual radio APs, you configure these settings for the 2.4GHz and 5GHz radios independently by going to **Configuration > Radio 2.4G** or **Configuration > Radio 5G**.

Figure 29. The Configuration > Wireless > Common page



To configure the wireless settings common to all WLANs

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a ZoneFlex 7363/7962, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Make changes to the common wireless settings listed in the table below.

Setting	Description
Radio Network	(Dual radio APs only) Allows you to change the name of the 2.4GHz and 5GHz radios (default: "Radio 2.4G" and "Radio 5G").

Wireless Mode	**On 802.11b/g APs:** The wireless mode options include the following: • *Auto-Select*: Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting. • *2.4GHz 54 Mbps (For faster 802.11g devices only)*: Allows only 802.11g-compliant devices to join the network. • *2.4GHz 11Mbps (For slower 802.11b devices only)*: Allows only 802.11b-compliant devices to join the network. **On dual radio 802.11n APs:** On dual radio 802.11n APs, the wireless mode is determined by radio; i.e., for the 2.4GHz radio, the mode is set to 2.4GHz (802.11b/g/n), while for the 5GHz radio, the mode is set to 5GHz (802.11a/n).
Channel	This option lets you select the channel used by the network. You can choose **SmartSelect**, or choose one of a specific number of channels. If you choose **SmartSelect**, the AP automatically selects the best channel (encountering the least interference) to transmit the signal.
Channel Width (11n APs only)	On 802.11n Access Points, the option to choose 40MHz channel width provides (theoretically) double the data capacity of the channel. However, wider channel width means fewer channels available, and more interference with other wireless signals.
Country Code	This option (if enabled) lets you select your country or region code.
Advanced Settings	Refer to "Reviewing Common Advanced Settings" on page 59.
AeroScout RFID	Select **Enabled** to enable AeroScout RFID tag detection.
External Antenna	*NOTE: This option only appears if you are using the ZoneFlex 2942 AP.* The ZoneFlex 2942 AP provides an external antenna port, in case you want to attach an external antenna to extend the range of your wireless network. To enable the AP to use the external antenna, select the **Enabled** option in this section. This option is disabled by default.

CAUTION: Selecting the incorrect country or region may result in violation of applicable laws. If you purchased the Access Point in the United States, you do not need to set the country code manually. Ruckus Wireless devices that are sold in the US are preconfigured with the correct country code and this setting is non-configurable.

3. If you are using AeroScout Tags in your organization to locate assets or personnel, you can use your ZoneFlex AP to relay location or presence data from the AeroScout Tags to the AeroScout Engine via Wi-Fi.

   To enable the AP to relay AeroScout data, click the **Enable** option in **AeroScout-RFID tag detection**.

   To check the status of the AeroScout communication agent (which relays location data from AeroScout Tags to the AeroScout Engine), go to the **Status > Wireless** page. Refer to "Viewing Current Wireless Settings" on page 91 for more information.

NOTE: For other AeroScout-related configuration, refer to the AeroScout documentation that was shipped with your AeroScout Tag and AeroScout Engine.

NOTE: If ZoneDirector exists on the network, you can enable AeroScout RFID tag detection on all its managed APs at once. Refer to the ZoneDirector online help for more information.

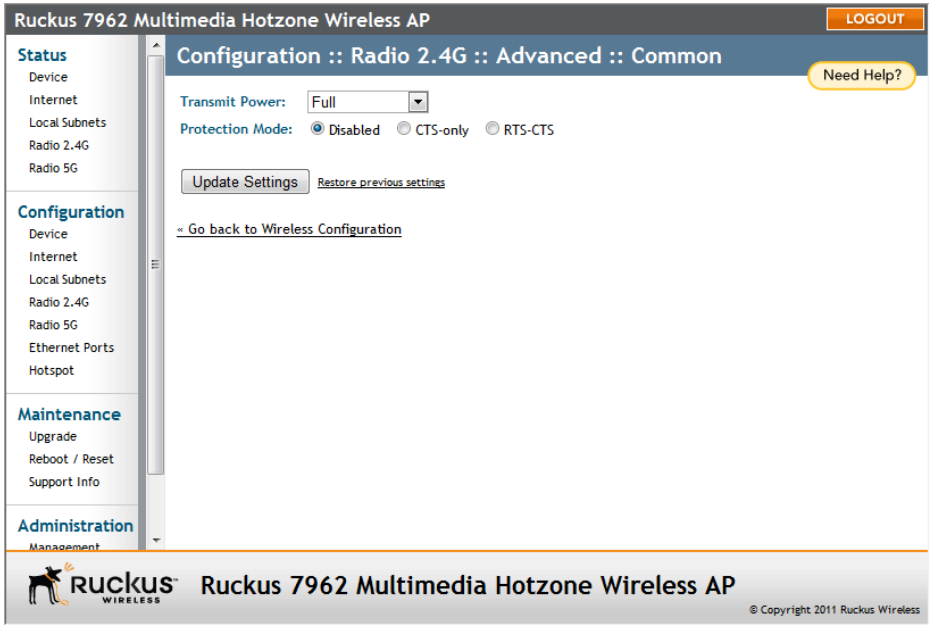
4. Click **Update Settings** to save your settings.

Reviewing Common Advanced Settings

Advanced wireless settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings be retained for best performance.

CAUTION: To fully benefit from the Access Point's capabilities, it is advisable not to change these values unless absolutely necessary.

Figure 30. The Configuration > Wireless > Advanced > Common page



To configure the advanced common options

1. On the **Configuration** > **Wireless** page, click **Edit Common Settings**. The *Configuration > Wireless > Advanced > Common* page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G > Edit Common Settings**.

2. Configure the advanced settings listed in Table 18 as required.

Table 18. Advanced wireless common settings

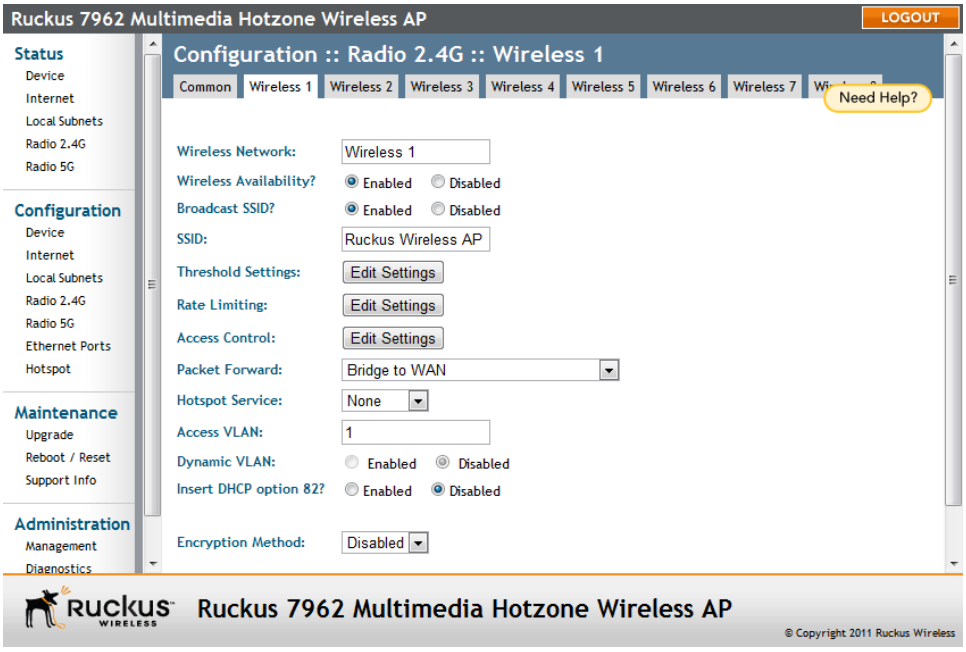
Option	Description
Transmit Power	The default setting is **Full**. Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the predefined power (this value differs according to the current country code).
Protection Mode	(Inactive by default.) If you activate protection, you control how 802.11 devices know when they should communicate with another device. This is important in a mixed environment of both 802.11b and 802.11g/11n clients. *WARNING: Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g/11n devices but will severely decrease performance.* • **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification. • **RTS/CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.

3. Click **Update Settings** to save and apply the changes.

Configuring Wireless # Settings

The Access Point provides up to eight wireless LANs per radio that can be individually configured to provide different kinds of services for different kinds of wireless clients, traffic types or different user groups. Each WLAN can be configured with separate security settings, VLANs, access controls and rate limiting policies, among other settings.

Figure 31. Wireless # settings



To configure wireless settings

1. Go to **Configuration** > **Wireless**. The *Configuration* > *Wireless* > *Common* page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click one of the eight **Wireless (#)** tabs. The *Configuration* > *Wireless* > *Wireless [#]* page appears.
3. Review the WLAN options listed in Table 19, and then make changes as required.

Table 19. WLAN options

Option	Description
Wireless Network	This wireless network name is for management purposes only, and is not visible to the user.
Wireless Availability	This option controls whether or not the wireless network is available to users (Off or On).
Broadcast SSID	This option controls whether or not the WLAN SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user to be told the correct SSID before they can connect to your network.
SSID	This is the publicly-broadcast "name" of your wireless network. SSIDs can contain up to 32 alphanumeric characters and are case-sensitive.
Threshold Settings	This button opens a page where you can configure the Protection Mode you activated on the *Configuration > Wireless > Advanced > Wireless [#]* page. If Protection Mode is not active, ignore this option. For more information, see "Setting Threshold Options" on page 70.
Rate Limiting	This button opens a page where you can configure upload and download limits per station. For more information, see "Rate Limiting" on page 72.
Access Control	This button opens a page where you can configure access controls for the WLAN. For more information, see "Controlling Access to the Wireless Network" on page 72.
Packet Forwarding	**Isolated**: Selecting Isolated causes the traffic from this WLAN to terminate at the Access Point. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this WLAN to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of wireless packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
Hotspot Service	Select a Hotspot configuration from the list to enable Hotspot service on this WLAN, if you have configured it from the Configuration > Hotspot page. See "Configuring Hotspot Service" on page 80.

Local Subnet	This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forwarding*, and allows you to choose which subnet this WLAN's traffic will be part of. You must have previously configured a subnet from the *Configuration > Local Subnets* page before it becomes available here.
Access VLAN	Enter a VLAN ID to segment all traffic arriving from this WLAN to a specified VLAN. Default is 1.
Dynamic VLAN	This setting is available only with WPA encryption and 802.1X authentication. Dynamic VLAN allows the dynamic assignment of VLANs to clients based on RADIUS attributes. Enable this option only if your RADIUS server is configured to segment clients using dynamic VLAN.
DHCP Option 82	When this option is enabled on an SSID, the SSID will be inserted into the DHCP request packet's Agent Circuit sub-option, and the AP's base MAC address will be inserted as the Agent Remote ID sub-option.
Encryption Method	By default, all data exchanges on your wireless network are not encrypted, but you can select an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption settings. *Ruckus Wireless strongly recommends using WPA as the encryption method as WEP has been proven to be easily circumvented.* For more information, see either "Using WEP" on page 64 or "Using WPA" on page 66.

4. When you are finished, click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.
5. Click **Go back to Wireless Configuration** to reopen the previous page.

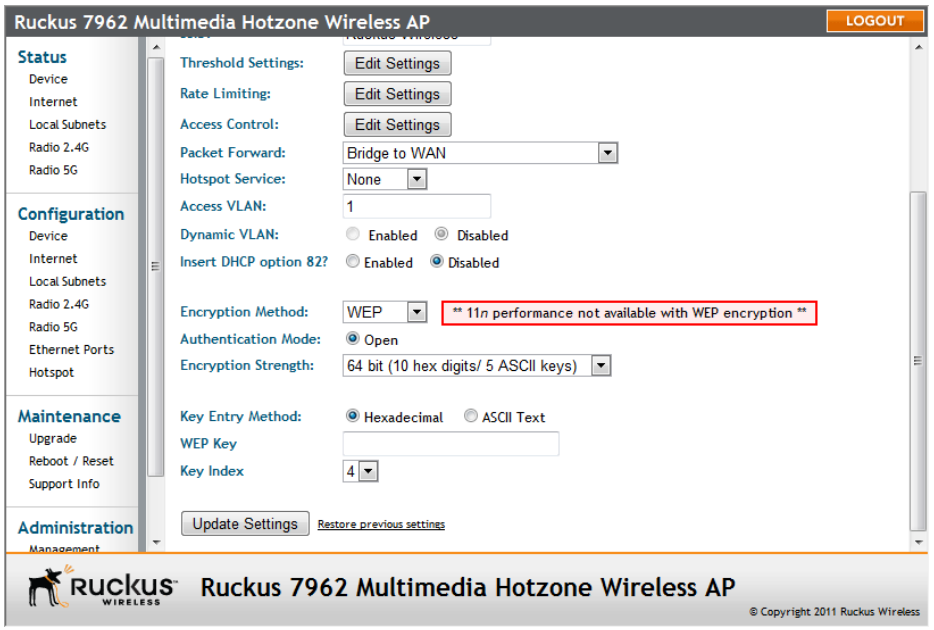
Using WEP

Wired Equivalent Privacy (WEP) is a security algorithm for 802.11 wireless networks designed to provide data confidentiality comparable to that of a wired network. WEP uses a pre-shared key for encrypting data frames that is shared among all users of the wireless network. For this reason and others, WEP has been discredited as a security mechanism and should be avoided in favor of WPA if at all possible.

CAUTION: WEP encryption has been proven to be easily circumvented. Therefore, Ruckus Wireless recommends using WPA whenever possible, and only use WEP if your client devices do not support WPA.

CAUTION: Using WEP encryption limits the performance of the AP to 802.11g rates. If you select WEP encryption for a WLAN, wireless devices that are capable of faster 802.11n transfer rates will be limited to 802.11g rates.

Figure 32. WEP settings



To configure WLAN-specific WEP encryption settings

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the **Wireless #** tab that you want to configure. The Configuration > Wireless > Wireless[#] page appears.
3. Click the **Encryption Method** menu, and then click **WEP**. An additional set of WEP-specific encryption options appear on this page.
4. Review the encryption settings listed in Table 20, and then make changes as required.

Table 20. WEP Options

Encryption Setting	Description

Authentication Mode	Open is the only authentication mode available with WEP encryption.
Encryption Strength	• 64 bit: Specify the key with 10 hexadecimal digits or 5 ASCII characters. • 128 bit: Specify the key with 26 hexadecimal digits or 13 ASCII characters. The 128-bit cryptography is stronger privacy protection for your network and is recommended if you use WEP.
Key Entry Method	• Hexadecimal: The encryption key only accepts hexadecimal characters (0-9, A-F). • ASCII Text: The encryption key accepts ASCII characters.
WEP Key	Enter the key manually according to the Key Entry Method and Encryption Strength settings.
Key Index	Choose the index, from "1" to "4", that the WEP key is to be stored in.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.
6. Click **Go back to Wireless Configuration** to reopen the previous page.

Using WPA

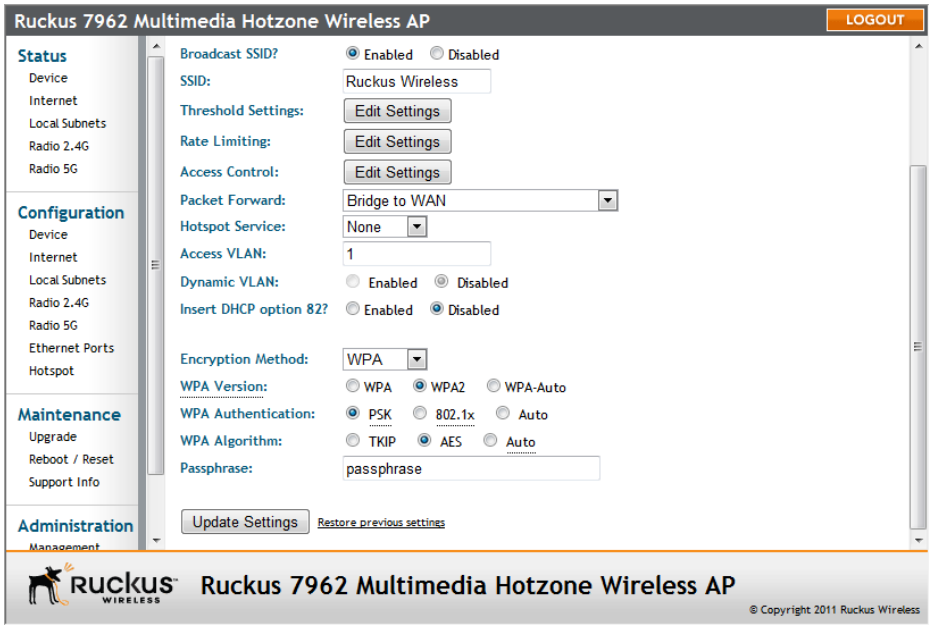
Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols developed by the Wi-Fi Alliance in response to the weaknesses of WEP.

Selecting WPA as the Encryption Method allows you to choose WPA version, WPA Authentication and WPA Algorithm. This section discusses WPA-PSK (pre-shared key). For information on WPA-Enterprise (WPA-802.1X), see "Customizing 802.1X Settings" on page 69.

Use of WPA-PSK (also known as WPA-Personal) allows automatic key generation based on a single passphrase. WPA-PSK provides strong security for home and small offices and does not require a RADIUS server, but may not be supported on older wireless devices. In some cases, the older devices can be upgraded with adapters to take advantage of WPA-PSK.

If you configure the WLAN with WPA-PSK, wireless users will not be able to connect to your WLAN unless their devices support WPA-PSK and are configured with the same passphrase.

Figure 33. WPA settings



To configure WPA encryption settings

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the Wireless # tab that you want to configure. The Configuration > Wireless > Wireless[#] page appears.
3. Click the **Encryption Method** menu, and then click **WPA**. An additional set of WPA-specific options appear on this page.
4. Review the encryption settings listed in Table 21, and then make changes as preferred.

Table 21. Encryption settings

Encryption Setting	Description
WPA Version	Your options are WPA, WPA2 or WPA Auto. • **WPA** (Wi-Fi Protected Access) is the replacement security standard adopted by the Wi-Fi Alliance in response to the security weaknesses of WEP. WPA was developed as an interim measure prior to the ratification of the 802.11i standard, which introduced WPA2. • **WPA2** provides stronger wireless security than WPA and is the recommended option. However, older wireless clients may not be compatible with WPA2. For example, WPA2 support on Windows XP requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later. • **WPA-Auto** allows both WPA and WPA2 devices to operate on the same WLAN.
WPA Authentication	**PSK** (Pre-Shared Key) mode is suitable for home or personal use. **802.1X** mode uses a RADIUS server to verify user identity. The auto mode offers both options for the wireless client to choose from. For more information on how to configure the 802.1X mode, refer to "Customizing 802.1X Settings" on page 69.
WPA Algorithm	• **TKIP**: Temporal Key Integrity Protocol is an older encryption algorithm that provides stronger security than a shared WEP key, but not as strong as the newer AES algorithm. • **AES**: AES (Advanced Encryption Standard) replaces TKIP as the default (and recommended) encryption algorithm for modern wireless LANs. • **Auto**: Auto allows both encryption algorithms to be used on the same WLAN. When Auto is selected, the wireless client decides whether TKIP or AES will be used. Note however that allowing TKIP will reduce the performance of the WLAN (as broadcast packets will be limited to slower transfer rates), and is therefore not recommended.
Passphrase	Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

6. Click **Go back to Wireless Configuration** to reopen the previous page.

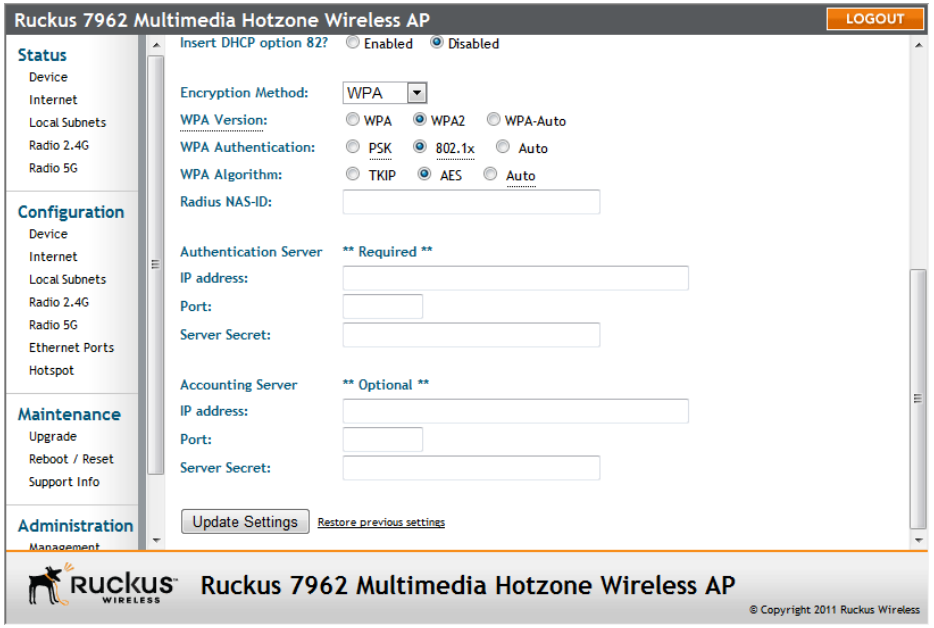
Customizing 802.1X Settings

CAUTION: Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

If you choose WPA as the encryption method, you have the option to set up the Access Point to act as an 802.1X proxy, utilizing external authentication sources such as a RADIUS server.

In 802.1X authentication, the supplicant sends access request messages along with credentials, such as user name / password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification. The supplicant (client device) remains in an unauthorized state until verification has been received. In unauthorized state, only 802.1X traffic is allowed; all other traffic, such as DHCP and HTTP traffic, is dropped. For its wireless interfaces, the Access Point can serve as the authenticator communicating between the supplicant and the authentication server.

Figure 34. 802.1X settings



To configure 802.1X authentication settings on a WLAN

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click a **Wireless #** tab to configure. The Configuration > Wireless > Wireless[#] page appears.
3. Click the **Encryption Method** menu, then click **WPA**. The basic set of WPA-specific encryption options appears on the page.
4. Select **802.1X** as the WPA Authentication mode. Additional options appear.
5. Configure the following settings to customize your 802.1X authentication:
   - **RADIUS NAS-ID**: Enter the network ID assigned to your RADIUS server.
   - **Authentication Server [-Required-]**: Enter the information needed to establish a connection between the Access Point and the RADIUS server.
   - **Accounting Server [-Optional-]**: Enter the information needed to establish this connection.
6. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.
7. Click **Go back to Wireless Configuration** to reopen the previous page.

Setting Threshold Options

The following options allow you to fine-tune the "Protection Mode" behavior, set previously on the *Configuration > Wireless > Advanced > Common* page. After activating a Protection Mode, you can open each Wireless tab and customize the threshold settings, which determine what is put into effect and when.

CAUTION: Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

To customize Protection Mode (Threshold) settings

1. Go to **Configuration > Wireless**. The *Configuration > Wireless > Common* page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the tab for the Wireless # (WLAN) that you want to configure. The *Configuration > Wireless > Wireless [#]* page appears.
3. Look for **Threshold Settings**, and then click **Edit Settings**. The *Configuration > Wireless > Advanced > Wireless [#]* page appears.
4. Review the options listed in Table 22, and then make any needed changes.

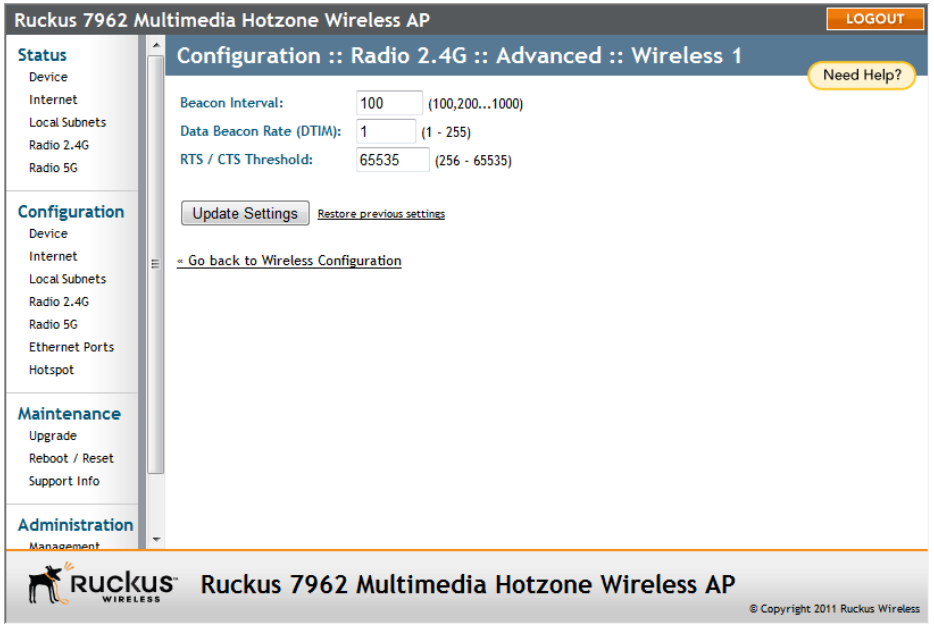
Table 22. Threshold options

Option	Description
Beacon Interval	(The default value is 100.) The value indicates the frequency interval of the beacon in milliseconds. A beacon is a broadcast packet sent by the AP to synchronize the wireless network.
Data Beacon Rate	(The default value is 1.) The value indicates the interval of the Delivery Traffic Indication Message (DTIM). This is a countdown field that the device uses to inform its clients of the next window for listening to broadcast or multicast messages.
RTS/CTS Threshold	(The default value is 65535.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in an environment with excessive signal noise or hidden nodes, but may result in some performance degradation.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

You have completed configuring the threshold options. To reopen the previous page, click the **Go back to Wireless Configuration** link.

Figure 35. Threshold settings



Rate Limiting

Rate Limiting allows you to cap the per client data transfer rates for a specific WLAN.

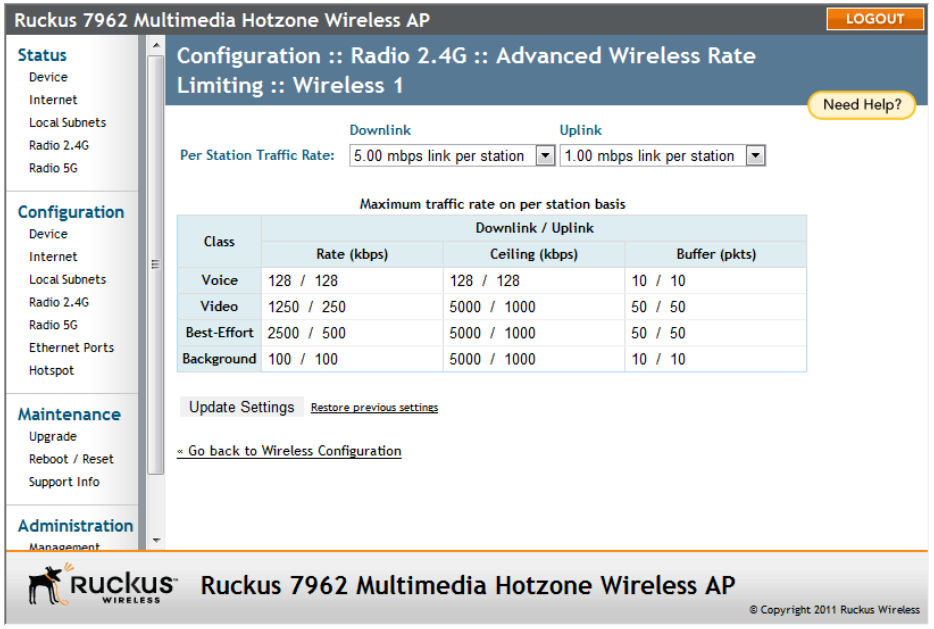
To enable per station rate limits

1. Go to **Configuration > Wireless**.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Select the WLAN that you want to configure from the tabs at the top of the page.
3. Click the **Edit Settings** button next to *Rate Limiting*. The *Rate Limiting* page appears.
4. Set the maximum **Downlink** and **Uplink** rate per station.
5. The table below updates to show the maximum transfer rate per station for each traffic type.
6. Click **Update Settings** to save your changes.

Figure 36. Limit per station traffic rates on a specific WLAN



Controlling Access to the Wireless Network

Access Control enables you to specify the stations are allowed to join (associate with) your wireless networks. Access controls can be configured for each WLAN from its respective *Wireless #* tab.

Access Control Options

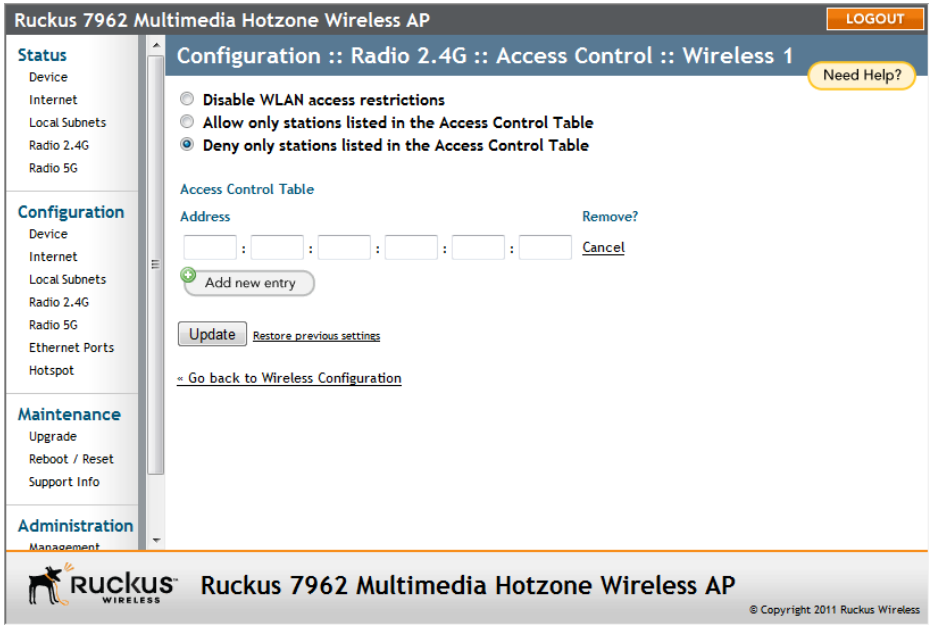
This section describes the options that you can use to control access to the wireless network.

- **Disabling WLAN Access Restrictions**: If you select **Disable WLAN access restrictions**, then MAC-address-based restrictions on which stations can join the WLAN are disabled; thus, any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption passphrase. The Access Controls table is hidden if the current mode is **Disable WLAN access restrictions**.
- **Allowing Only Stations Listed in the Access Controls Table**: If you select **Allow only stations listed in the Access Controls Table**, then stations entered into the access-controls table are allowed but all others are disallowed. To add MAC addresses, see "Changing the Access Controls for a WLAN" on page 73.
- **Denying Only Stations Listed in the Access Controls Table**: If you select **Deny only stations listed in the Access Controls Table**, then stations entered into the access-controls table are disallowed but all others are allowed. To add MAC addresses, see "Changing the Access Controls for a WLAN" on page 73.

Changing the Access Controls for a WLAN

By default, the **Disable WLAN access restrictions** option is selected, which allows any wireless station to gain access to the wireless network. If you want to change this setting, follow the instructions below.

Figure 37. Access control settings



To edit the ACL

1. Go to **Configuration** > **Wireless**.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the **Wireless #** tab for which you want to configure the access control settings.
3. Click the **Edit Settings** button next to *Access Control*.
4. Select the radio button for the desired access control. (For a description of the options, see "Access Control Options" in the previous section.) The Access Controls Table appears.
5. To add a MAC address to the Access Control table, click the **Add new entry** button.
6. Fill out the following text boxes:
   - **Address**: Six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. You can specify a full 12-hex-digit MAC address or enter "wildcard" characters for "don't care" digits. Allowable hex-digit characters are 0-9, a-f, and A-F. Most address-tags and software where you find MAC addresses listed include colons or dashes to separate the address-pairs; that is provided for you on the web page, so do not enter the colons or dashes.

     Supported wildcard characters include "x", "X" and blank (space character). Wildcards are useful when you want to specify all MAC addresses from a given manufacturer. For example, by specifying only the Organizationally Unique Identifier (the first six hexadecimal digits of any MAC address from that manufacturer is its OUI) saves you having to enter all 24 million of them (the table size is limited in the AP/Router to 128 entries). Some manufacturers produce devices using more than one OUI, in which case you may need to enter each applicable one.
7. Click **Update** to save your changes. Assuming all parameters you entered are acceptable, that row will be added to the table.

You have completed adding an entry to the MAC address table. If you have additional MAC addresses you want included, click **Add new entry**, and then repeat these steps until you have entered all the stations you want. There is a limit of 128 rows.

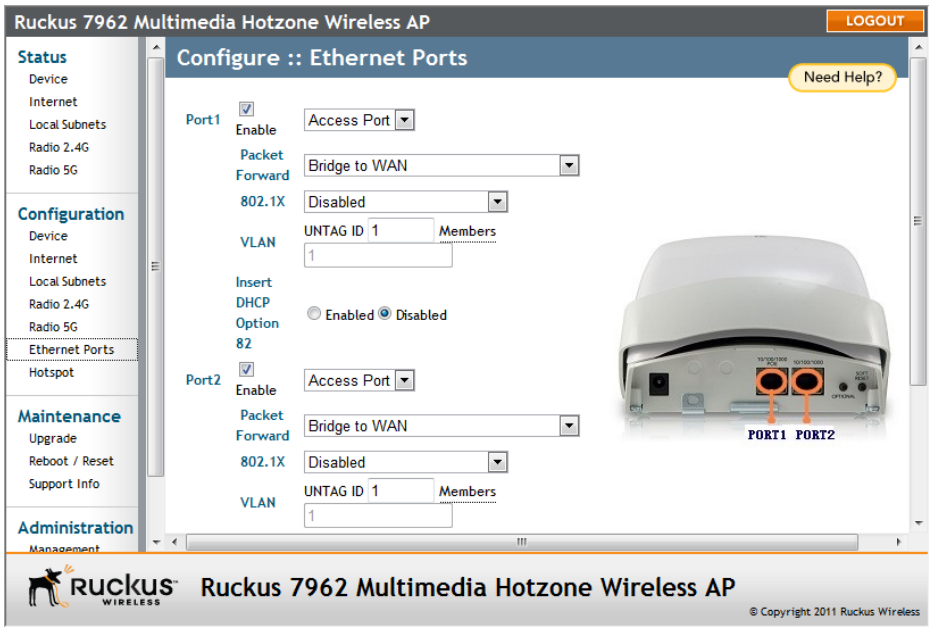
Removing a MAC Address

To remove a MAC address from the ACL table, click the **Cancel** button under the *Remove* column, and then click **Update**. The ACL table refreshes, and the MAC address that you deleted disappears from the table.

Configuring Ethernet Ports

The Ethernet Ports configuration page allows you to define how the Access Point's Ethernet ports behave. You can disable ports entirely, define trunking and packet forwarding behavior, configure 802.1X authentication settings, and configure VLAN settings for each port individually from this page.

Figure 38. The Configuration > Ethernet Ports page



To configure LAN ports

1. Go to **Configuration > Ethernet Ports**.
2. Review the following table and make changes as needed for each of the ports labeled **PORT 1** through **PORT 4** (depending on AP model), which correspond to the AP's Ethernet ports.

Setting	Description
Enable	All Ethernet ports are enabled by default. Unchecking this box next to a port disables that port entirely. If you do not want to provide wired access through the AP, uncheck (clear) the **Enable** box next to each LAN port.

Port Type	See "Setting Ethernet Port Type" on page 77 for more detailed information. ■ **Trunk port**: This port passes all VLAN traffic. ■ **Access Port**: This port provides network access. ■ **General Port**: User-defined VLAN membership.
Packet Forwarding	**Isolated**: Selecting Isolated causes the traffic from this port to terminate at the Access Point. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this port to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
802.1X	Configure the port as an 802.1X authenticator or supplicant. The following options are available: ■ **Disabled**: No 802.1X controls are applied to this port. ■ **Authenticator (Port-based)**: Only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. ■ **Authenticator (MAC-based)**: Each MAC host is individually authenticated. ■ **Supplicant**: The port acts as a supplicant to an upstream authenticator. Configure a port as Supplicant if the port is a Trunk Port used to connect the AP to a LAN switch. See "Working with 802.1X on Wired Ethernet Ports" on page 78 for more information.

VLAN	**Untag ID**: Enter a valid VLAN ID in this field to segment traffic arriving on this port to a specific VLAN. Default is 1. Valid VLAN entries are 1-4094. **Members**: Displays the VLAN membership of the port. (Membership is configurable only for the General port type.) See "Working with Port-Based VLANs" on page 80 for more information.
Insert DHCP Option 82	When this option is enabled for an Ethernet port, the AP's base MAC address and device name will be inserted as the Agent Remote ID sub-option for DHCP request packets. This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

3. Click **Update Settings** to save your changes.

Setting Ethernet Port Type

ZoneFlex AP Ethernet ports can be configured as one of the following port types:

- Trunk Port
- Access Port
- General Port

Trunk Port

Trunk Ports forward and receive tagged and untagged frames and are used for bridging switch ports together. The Trunk port is a member of all VLANs that exist on the switch, and all VLAN-tagged traffic arriving on the port is seen. If an untagged frame is received on a Trunk port, the frame is associated with the Untag VLAN (also known as "native VLAN", by default, 1).

If a port is configured as a Trunk port, the Untag ID field can be used to define the Untag VLAN--the VLAN that the switch uses for forwarding/filtering purposes when a frame arrives without an 802.1Q header.

Access Port

Access Ports are used to provide network access. Traffic arriving on different Access Ports can be segmented into different logical networks (VLANs) using the Untag VLAN ID field. Access Ports are members of only one VLAN--the VLAN that is configured in the Untag VLAN field.

General Port

The General Port can be configured to support multiple tagged VLANs and one untagged VLAN. As Trunk Ports by definition are members of all VLANs, the General Port is the only port type for which membership is user configurable.

Working with 802.1X on Wired Ethernet Ports

802.1X authentication consists of the following three components:

- *Supplicant*: The supplicant sends access request messages along with credentials, such as user name / password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification.
- *Authenticator*: The authenticator challenges the identity of the supplicant, then passes its credentials to the AAA server. If the credentials are accepted the supplicant is allowed access.
- *Authentication Server (AAA Server)*: The AAA server verifies the supplicant's credentials and permits or rejects its request for access.

For wired 802.1X, a Ruckus AP's Ethernet port can be configured as either an *Authenticator* or as a *Supplicant*, depending on which port type is selected. Table 23 and Table 24 describe the 802.1X roles available by port type.

Table 23. Authenticator support by port type

	Trunk Port	Access Port	General Port
Port-based mode	X	X	X
MAC-based mode		X	

Table 24. Supplicant support by port type

	Trunk Port	Access Port	General Port
Supplicant	X		

The following considerations apply:

- A single port can not be configured as both an *Authenticator* and *Supplicant* at the same time.
- Only one port per AP can be configured as a *Supplicant*.
- If the AP is connecting to a switch port with 802.1X authentication enabled, the AP's port type should be configured as a Trunk Port and its role should be configured as *Supplicant*. The switch port should be configured as a Trunk port in *Port-based Authenticator* mode.

- If there are multiple devices connected to an AP port (through a downstream switch), the port can be configured as either *Port-based* or *MAC-based Authenticator*. In Port-based mode, only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. In MAC-based mode, each MAC host is individually authenticated.
- If a Trunk Port is configured as a *Supplicant*, a user name and password must be entered to authenticate the port to the 802.1X aware LAN switch.
- If an Access Port is configured as an *Authenticator*, the administrator must define the RADIUS server that the Authenticator will communicate with. All Ethernet ports of a single AP are configured with the same RADIUS server.

Enable MAC authentication bypass: If MAC authentication bypass is enabled, the port first attempts to authenticate the attached device by MAC address, and if that fails, it will try to authenticate the device using 802.1X.

Working with Port-Based VLANs

The Access Point provides options for segmenting all incoming traffic (both wireless and wired Ethernet traffic) into specific VLANs. There are two ways to segment incoming traffic into VLANs:

- Each of the wireless interfaces (SSIDs) can be configured with a specific Access VLAN ID: (**Configuration > Wireless > Wireless [#] > Access VLAN**).
- Each of the LAN ports can be configured with an Untag VLAN ID (**Configuration > Ethernet Ports > VLAN > Untag ID**).

For Ethernet ports, the behavior of the Untag VLAN ID depends on the Port Type selected. If the port is configured as a Trunk port, it will include all VLANs (1-4094) in its membership. The VLAN Untag ID field (default = 1) can be used to redefine the "Native VLAN" for the port.

If the Ethernet port is configured as an Access Port, it can be configured with only one Untag VLAN ID and its membership includes only that one VLAN.

If the Ethernet port is configured as a General Port, it can be configured to include multiple VLANs in its membership and one Untag VLAN.

Configuring Hotspot Service

Hotspot service can be deployed on standalone ZoneFlex APs through the Web interface. At a minimum, you must configure a login redirect URL and a RADIUS server to which users will be authenticated. Additional options and controls are provided on subsequent pages.

To enable Hotspot service

1. Go to **Configure > Hotspot**.
2. Click **Enabled** next to *Hotspot Service*.
3. Review the settings in table Table 25, and make changes as needed.

Table 25. Hotspot configuration settings

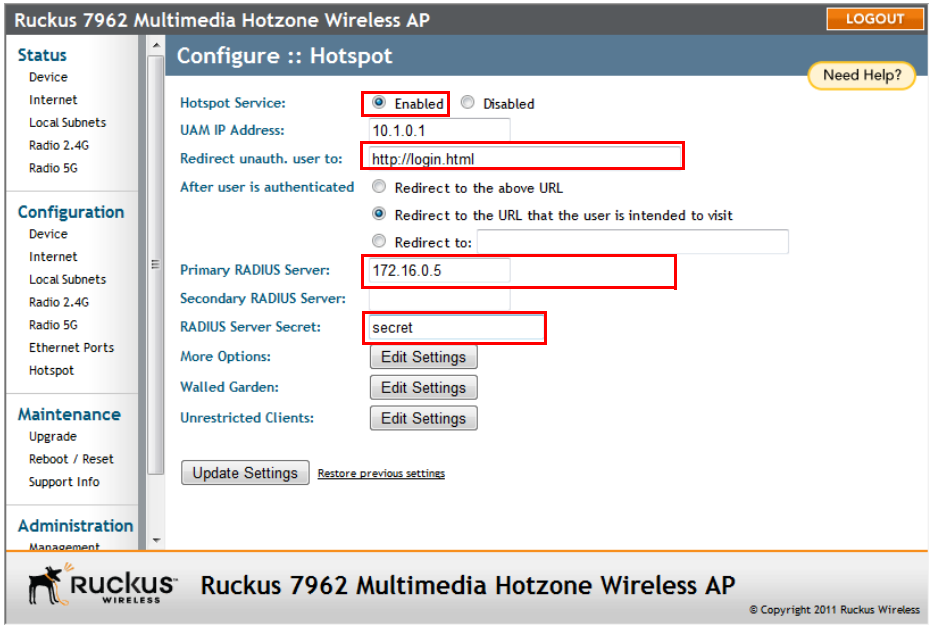
Setting	Description
UAM IP Address	Specify the IP address of the UAM service.
Redirect unauth. user to	Redirect unauthenticated users to the specified URL (login page).

Setting	Description
After user is authenticated	Select where you want to redirect the user after successful authentication. • *Redirect to the above URL*: return to the login URL configured above. • *Redirect to the URL the user intended to visit*: upon successful authentication, go directly to the URL that the user originally entered (typically the browser's home page). • *Redirect to*: specify a URL to which users are redirected after authentication. This can be used to redirect users to a "Login Successful" page, or a page that offers connection time information or a Logout button.
Primary RADIUS Server	Enter the IP address of the primary RADIUS server against which users will be authenticated (required).
Secondary RADIUS Server	Enter the IP address of the secondary RADIUS server, if one is available (optional).
RADIUS Server Secret	Enter the shared secret for communication with the RADIUS server (required).

4. Click **Update Settings** to save your changes.

You have completed the minimum settings for providing Hotspot service on this AP. Additional configuration options are available using the *Edit Settings* buttons at the bottom of the page.

Figure 39. Minimum configuration settings for providing Hotspot service



Customizing Hotspot Optional Settings

Optional Hotspot settings include a number of options for fine-tuning your Hotspot service, such as maximum session time, grace period, accounting update interval, etc.

The following Hotspot options can be configured from the *Configure* > *Hotspot* > *More Options* page:

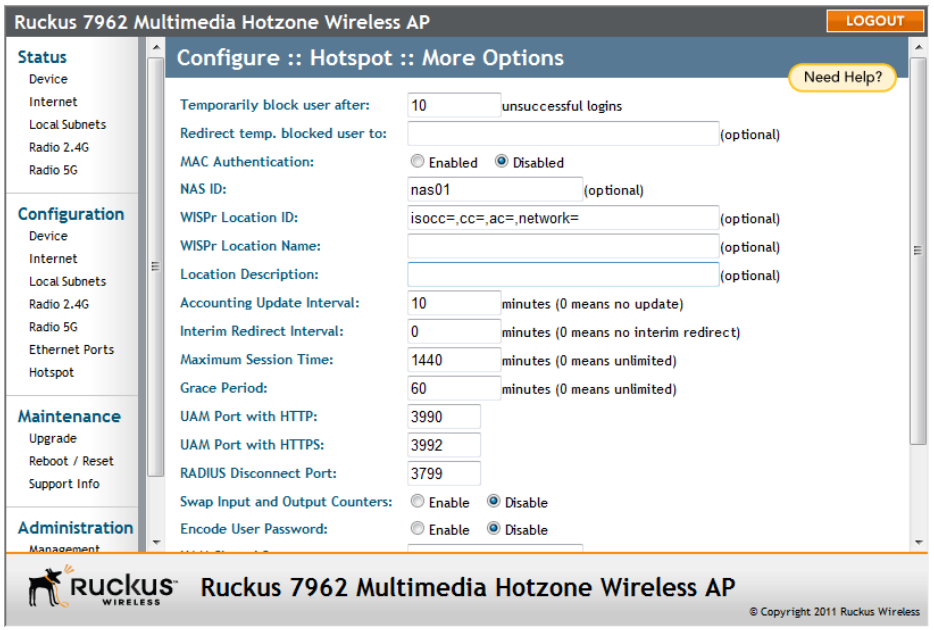
Table 26. Optional Hotspot settings

Setting	Description
Temporarily block user after __ unsuccessful login attempts	Specifiy the maximum number of repeated authentication failures allowed.
Redirect temp. blocked user to	Enter a redirect URL to which blocked users will be redirected.
MAC Authentication	If enabled, the Hotspot service will attempt to authenticate users based on their MAC addresses if the local Hotspot authentication has failed. If enabled, an optional MAC authentication password can be entered. If no password is specified, the system will use the client's MAC address as the password.

NAS ID	Specify the Network Access Server identifier of this device. The NAS-ID attribute is sent in RADIUS access and accounting request messages. It can also be used as location identification when NAS-IP-Address cannot be used for this purpose.
WISPr Location ID	Specify the Hotspot location identifier. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of "isocc=<ISO_Country_Code>, cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>".
WISPr Location Name	Specify the hotspot location and operator's name. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of "<HOTSPOT_OPERATOR_NAME>,<Location".
Location Description	Specify the description of location. This value is provided in the HTTP redirection.
Accounting Update Interval	Specify the interval for RADIUS accouting requests.
Interim Redirect Interval	Specify the interval after which users will be redirected to the login URL.
Maximum Session Time	Enter the maximum session time in minutes.
Grace Period	Specify the maximum time that a user may disconnect from the Hotspot service and return without the need to login again.
UAM Port with HTTP	TCP port to bind to for authenticating clients using HTTP.
UAM Port with HTTPS	TCP port to bind to for authenticating clients using HTTPS.
RADIUS Disconnect Port	UDP port to listen to for accepting RADIUS disconnect requests.
Swap Input and Output Counters	Swap the value of input counters (packets, octets and giga words) and output counters in RADIUS accounting requests. This option is mainly for backward compatibility with existing Chillispot deployments.
Encode User Password	Encode user password with challenge string, if UAM secret is not specified; otherwise, encode user password with both challenge string and UAM secret.

UAM Shared Secret	The UAM Shared Secret is the shared secret between this Access Point and the HTTP server for the Redirection URL. This setting is optional.

Figure 40. The Configure > Hotspot > More Options page



Creating a Hotspot Walled Garden

You can use the Hotspot Walled Garden rules to designate network destinations (host address or subnet) that users can access without going through authentication. A Walled Garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the Walled Garden. URLs will be resolved to an IP address (up to four). Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to reauthenticate when they navigate through the page.

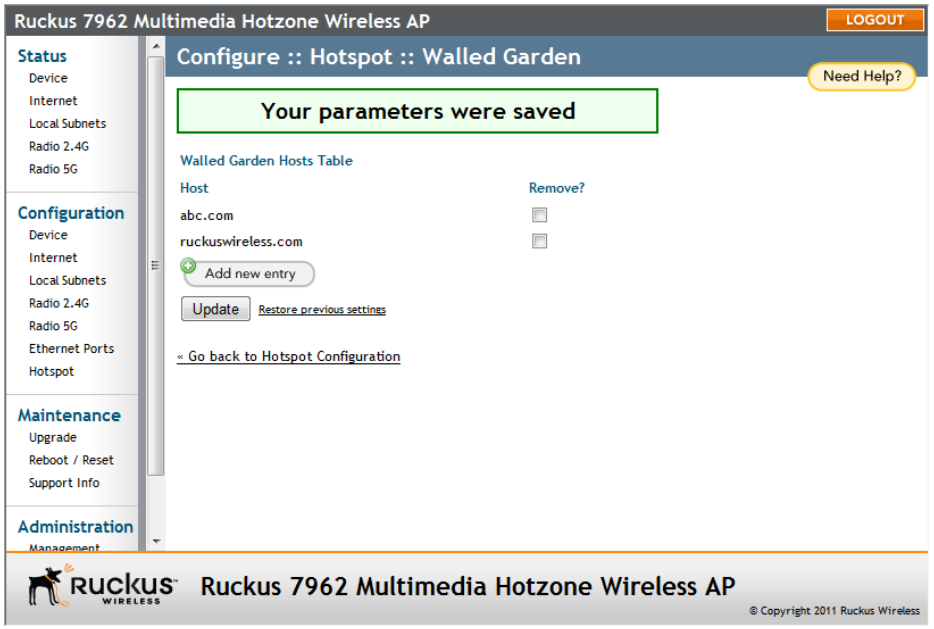
To create Walled Garden rules

1. Go to **Configure > Hotspot > Walled Garden**.
2. Click **Add New Entry**. A field entitled *Walled Garden Hosts* appears.
3. In *Walled Garden Host*, enter a host name, IP address, network segment (e.g., 192.168.1.0/24) or a domain name. If a domain name is entered, it will be resolved every 5 minutes.

4. Click **Update** to save your entry.

You can create up to 64 entries in the Walled Garden Hosts table.

Figure 41. The Walled Garden hosts table



To remove entries from the Walled Garden hosts table

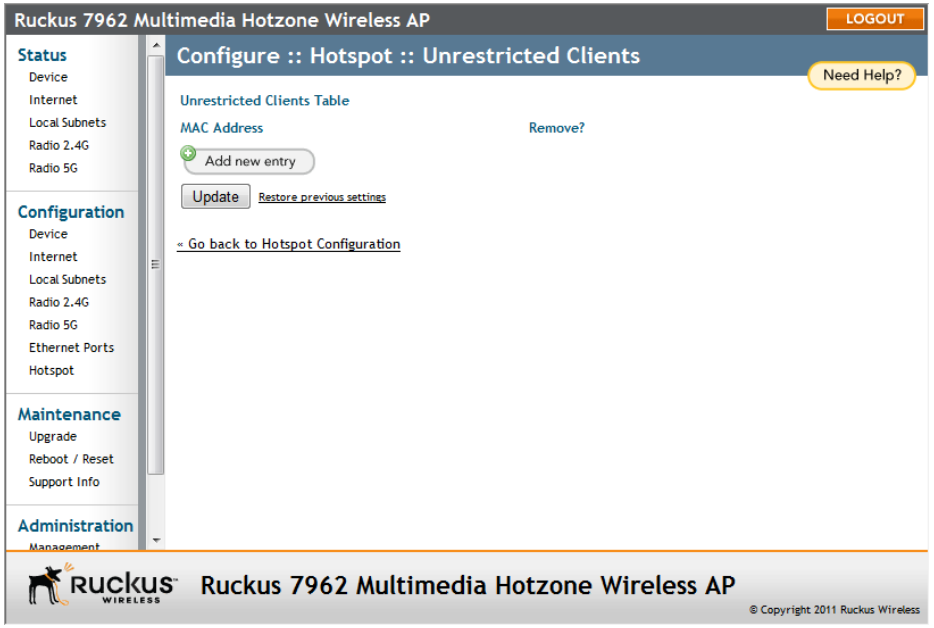
1. Click the check box next to the entry you want to remove, under the **Remove?** column.
2. Click **Update**. The entry is removed from the list.

Allowing Unrestricted Access by MAC Address

To allow certain clients unrestricted access to your Hotspot service

1. Go to **Configure > Hotspot > Unrestricted Clients**.
2. Click **Add New Entry**, and enter the MAC address of each client in the fields provided.
3. Click **Update** to save your changes.

Figure 42. Configuring Hotspot unrestricted clients table



5

Managing the Access Point

In This Chapter

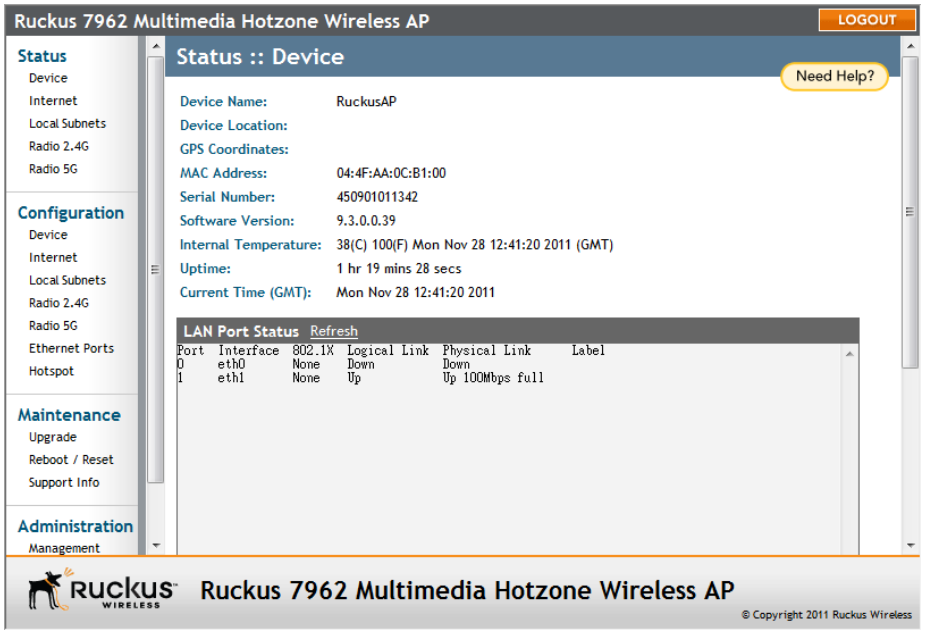
Viewing Current Device Settings 88
Viewing Current Internet Connection Settings 89
Viewing Current Local Subnet Settings 90
Viewing Current Wireless Settings 91
Viewing Associated Wireless Clients 92
Changing the Administrative Login Settings 93
Enabling Other Management Access Options 94
Working with Event Logs and Syslog Servers 100
Upgrading the Firmware 102
Rebooting the Access Point 104
Resetting the Access Point to Factory Defaults 105
Running Diagnostics 106

This chapter provides instructions for managing standalone ZoneFlex Access Points using the Web interface. For information on managing your ZoneFlex network using ZoneDirector, refer to the ZoneDirector User Guide, available from the Ruckus Wireless website.

Viewing Current Device Settings

The Status > Device page displays a general overview of the AP's current status, including device name, serial number, MAC address, current software version, etc.

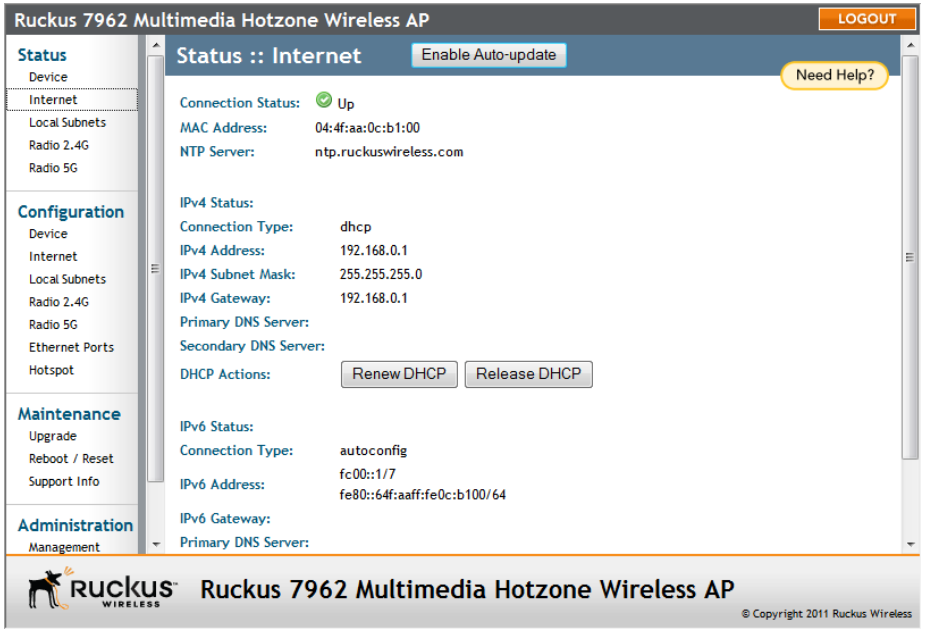
Figure 43. The Status > Device page



Viewing Current Internet Connection Settings

The Status > Internet page displays information on the AP's network settings; i.e., the settings that allow the AP to communicate with your local network and the Internet. Information includes IP address, gateway, DNS server, NTP server and connection type (method of obtaining an IP address -- DHCP or static IP).

Figure 44. The Status > Internet page

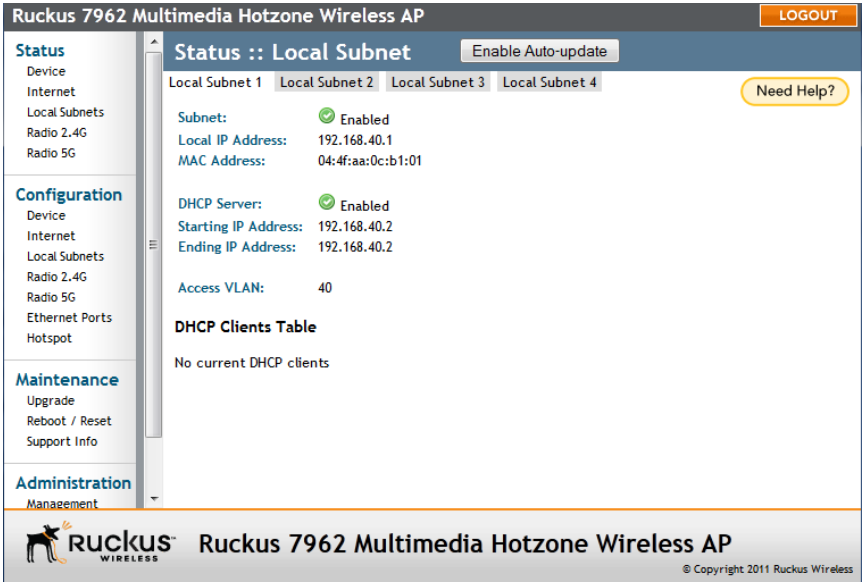


Viewing Current Local Subnet Settings

The Status > Local Subnets page can be used to view the router (local subnet) configurations and list of any clients connected to those subnets.

If you want to make changes to any of these settings, go to **Configuration > Local Subnets**. Refer to "Configuring Local Subnets" on page 55 for more information.

Figure 45. The Status > Local Subnet page



Viewing Current Wireless Settings

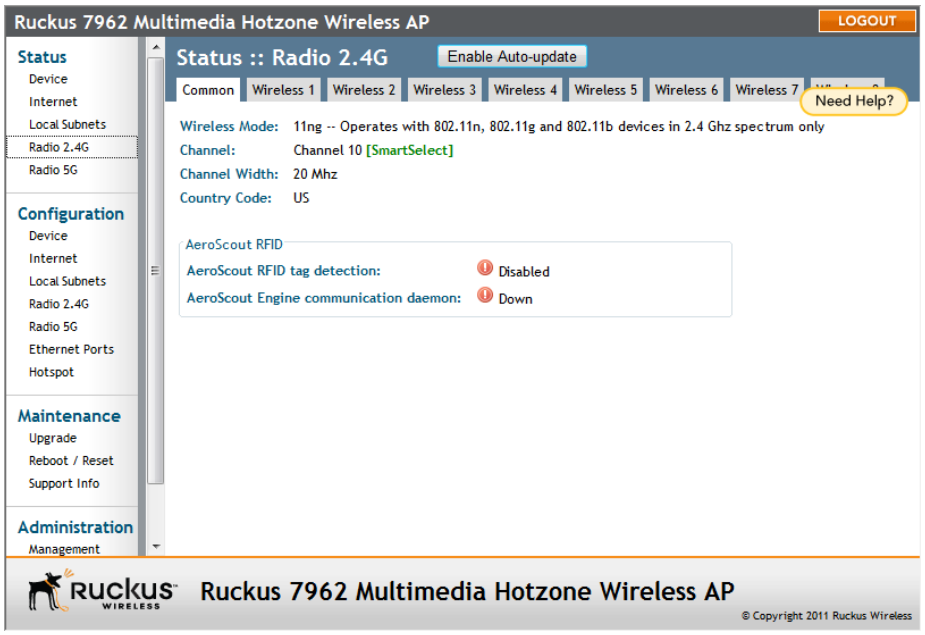
If you want to view the current common wireless settings that the AP is using, go to the **Status** > **Wireless** page (on dual band APs, go to **Status > 2.4G** or **Status > 5G**). Table 27 lists the descriptions of each common wireless setting.

Table 27. Common Wireless settings

Setting	Description
Wireless Mode	Shows the wireless mode that the AP is currently using. Possible values include: • Auto-Select • 2.4GHz 54 Mbps • 2.4GHz 11 Mbps • 11ng (Operates with 802.11n, 802.11g and 802.11b devices in 2.4 Ghz spectrum only) • 11na (Operates with 802.11n and 802.11a devices in 5 GHz spectrum only)
Channel	Shows the wireless channel that the AP is currently using. If you set the wireless channel to SmartSelect, this field will show the value **Channel # [SmartSelect]**.
Channel Width	11n devices only. Displays whether the channel width is set to 20MHz or 40MHz.
Country Code	Shows the country code that the AP has been set to use. *CAUTION: Verify that the AP is using the correct country code to make sure it uses only the allowed radio channels in your region. Selecting the incorrect country code may result in violation of application laws.*
AeroScout RFID tag detection	Shows **Enabled** if you enabled AeroScout RFID tag detection. The default setting is **Disabled**.
AeroScout Engine communication daemon	Shows **Up** if the communication agent on the AP is able to relay location data from AeroScout Tags to the AeroScout Engine. If the communication agent is unable to relay data or AeroScout tag detection is disabled, this field will show **Down**.

If you want to make changes to any of these settings, go to the **Configuration** > **Wireless** page. Refer to "Configuring Common Wireless Settings" on page 56 for more information.

Figure 46. The Status > Wireless (Radio 2.4G/5G) page



Viewing Associated Wireless Clients

A usage-monitoring capability has been built into the Access Point to help you monitor wireless clients that are associated with your wireless network.

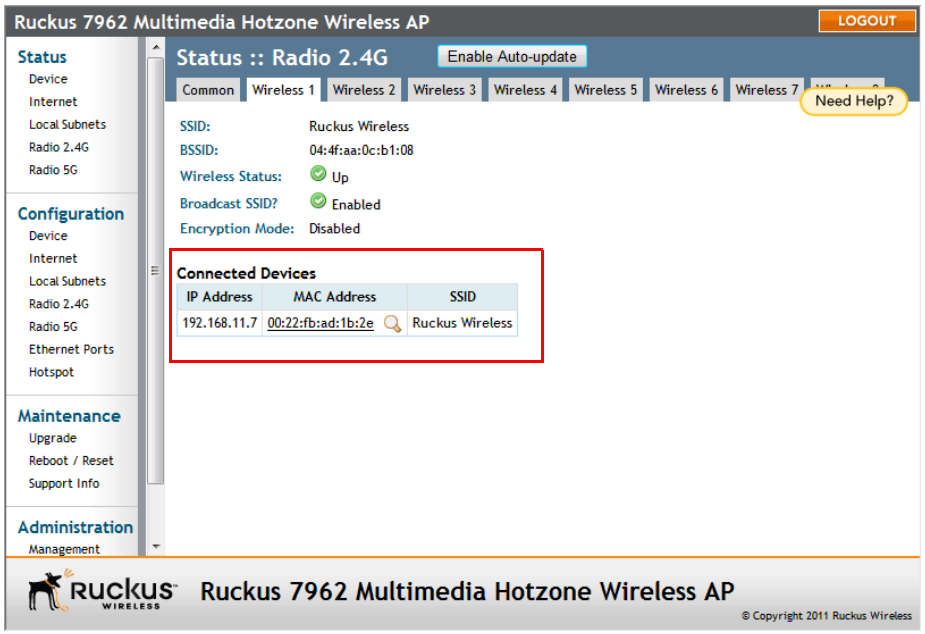
To view associated wireless clients

1. Go to **Status** > **Wireless**. The Status > Wireless page appears.

NOTE: If you are using a ZoneFlex 7363/7962 AP, go to **Status** > **Radio 2.4G** or **Status** > **Radio 5G.**

2. Click any of the **Wireless** tabs. Wireless clients that are associated with this particular wireless network appear under **Connected Devices**.

Figure 47. Viewing connected devices



Changing the Administrative Login Settings

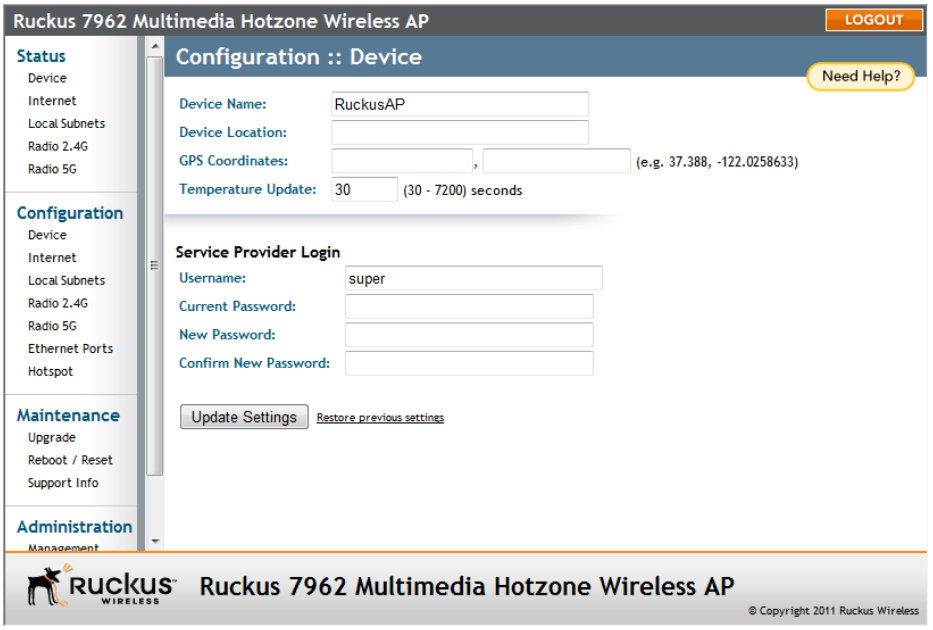
The default user name is `super` and the default password is `sp-admin`. To prevent unauthorized users from logging in to the Web interface using these default administrator login settings, Ruckus Wireless recommends that you change the default Web interface password immediately after your first login.

To change the default administrator login settings

1. Log into the Web interface.
2. Go to **Configuration** > **Device**. The Device page appears.
3. Under **Service Provider Login**, change the default administrator login settings.
   - In **Username**, type a new user name that you will use to log in to the Web interface. The default user name is `super`.
   - In **Password**, type a new password to replace the default password `sp-admin`. The password must consist of six to 32 alphanumeric characters only.
   - In **Password Confirmation**, retype the new password.
4. Click **Update Settings**. The message *Your parameters were saved* appears.

You have completed changing the default login settings. The next time you log in to the Web interface, make sure you use these updated login settings.

Figure 48. The Configuration > Device page



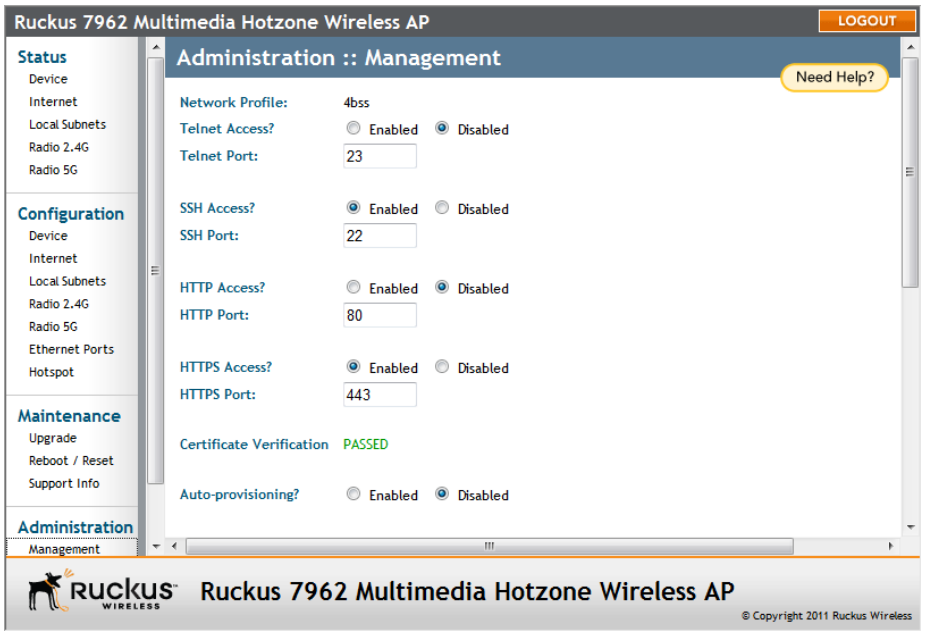
Enabling Other Management Access Options

In addition to managing the AP via a Web browser through HTTPS, several other management access options are available on the AP. These options include management access via HTTP, Telnet, and SSH.

You can also view and set up the connection to a Ruckus Wireless FlexMaster server under the **TR-069/SNMP Management Choice** options. If your ZoneFlex device is to be managed by FlexMaster, then the FlexMaster information (server URL and contact interval) is preconfigured before you receive your ZoneFlex device.

NOTE: If you are configuring the AP to be managed by FlexMaster, remember to point it to the FlexMaster server after you configure the management access options. For more information, refer to "Viewing FlexMaster Management Status" on page 98.

Figure 49. The Administration > Management page



To enable other management access options

1. Go to **Administration** > **Management**. The Management page appears.

2. Review the access options listed in Table 28, and then make changes as needed.

Table 28. Management Access Options

Option	Description
Telnet access	By default, this option is disabled (inactive).
Telnet port	This field lists the default Telnet port of 23 — only if Telnet is active. You can manually change this port number, if required.
SSH access	By default, this option is enabled (active).
SSH port	This field lists the default SSH port of 22—only if SSH is active. You can manually change this port number if required.
HTTP access	This option is disabled by default.
HTTP port	This field lists the default HTTP port of 80, if HTTP has been activated. You can manually change this port number if required.
HTTPS access	By default this option is enabled. This connection mode requires a security certificate, a copy of which has been pre-installed in the device.
HTTPS port	This field lists the default HTTPS port of 443—only if HTTPS has been activated. You can manually change this port number if required.
Certification Verification	This notes whether the security certificate linked to the HTTPS settings has been passed or not.
Auto-provisioning	This setting is disabled by default, and should only be enabled if using FlexMaster server for AP management.

3. If you want to use TR-069 or SNMP to manage the AP, configure the settings listed in Table 29.

Table 29. TR-069 and SNMP Management Options

Option	Description
Auto	Enables the ZoneFlex device to be managed by either SNMP server, Ruckus Wireless ZoneDirector, or Ruckus Wireless FlexMaster.
SNMP only	Only allow SNMP management
FlexMaster only	Only allow FlexMaster management
DHCP Discovery	URL of server providing DHCP

Table 29. TR-069 and SNMP Management Options

Option	Description
FlexMaster Server URL	URL of the FlexMaster server
Digest-authentication Username/Digest-authentication password	This information is automatically generated by the AP and used for authentication with FlexMaster. Change this value *only* if you want the AP to connect to another access control server (ACS).
Periodic FlexMaster Inform Interval	Interval at which the device should attempt to contact FlexMaster

4. Click **Update Settings** to save your changes. A confirmation message appears at the top of the page.

You have completed configuring the management access options.

NOTE: Remember to open any relevant firewall ports between the AP and the firmware upgrade/management server. For example, if HTTPS is used for firmware upgrades, open TCP port 443 on the firewall to allow connections through port 443. If FlexMaster server is used, open TCP ports 80 and 443 for HTTP/HTTPS communications, and TCP port 8082 for AP wake-up commands.

Viewing FlexMaster Management Status

If you configure the AP to be managed by FlexMaster, you can check the *TR-069 Status* section on the **Administration** > **Management** page.

Figure 50. TR-069 status information

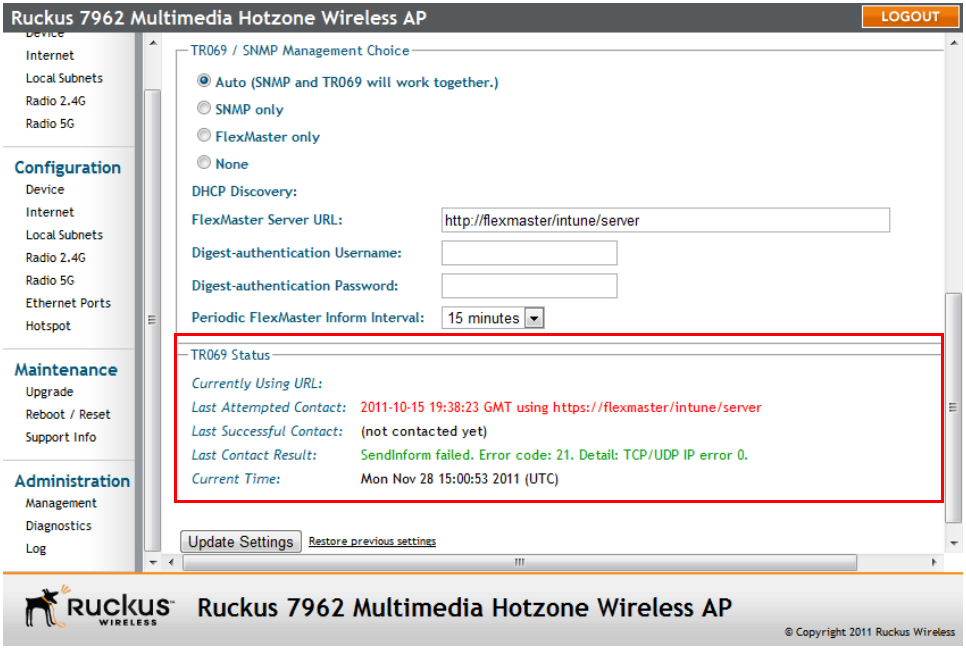


Table 30 lists the TR-069 status information that the AP provides.

Table 30. TR-069 status information

Status Information	Description
Currently using	Shows the FlexMaster server IP address or URL with which the AP is currently registered
Last attempted contact	Shows the date and time of the AP's last attempt to contact FlexMaster. Date and time are specified in GMT (or UTC), which are accurate if a Network Time Protocol (NTP) server is configured.
Last successful contact	Shows the date and time of the AP's last successful contact with FlexMaster.
Last contact result	Shows the result of the last attempt to contact FlexMaster (success or failure, and failure error code if applicable).
Current time	Shows the current date and time as known to the AP. This timestamp is accurate if an NTP server is configured on the AP. If there is no NTP server configured, this timestamp is useful as a reference for comparison of the timestamps for **Last attempted contact** and **Last successful contact**.

Pointing the AP to FlexMaster

Your ZoneFlex device is required to "call home" to register with your FlexMaster; FlexMaster does not initiate initial contact. To register successfully with FlexMaster, your ZoneFlex device must know the FlexMaster server's URL, thus entered on the device. You will need TCP ports 80 and 443 between APs and FlexMaster when traversing Layer 3/firewall boundaries.

To point the AP to FlexMaster

1. Go to **Administration > Management**.
2. Under **TR-069/SNMP Management Choice**, click **Auto**.
3. In **FlexMaster Server URL**, type the URL of the FlexMaster server.
4. Toggle the **Contact FlexMaster every** drop-down list to select how frequently the device will check the FlexMaster server for any pending configuration changes available for that ZoneFlex unit. On the FlexMaster side, this field is referred to as the Periodic Inform Interval.
5. Click **Update Settings** to save your changes.

After the AP registers with FlexMaster, this **Administration > Management** page will show the communication status between the AP and FlexMaster.

Working with Event Logs and Syslog Servers

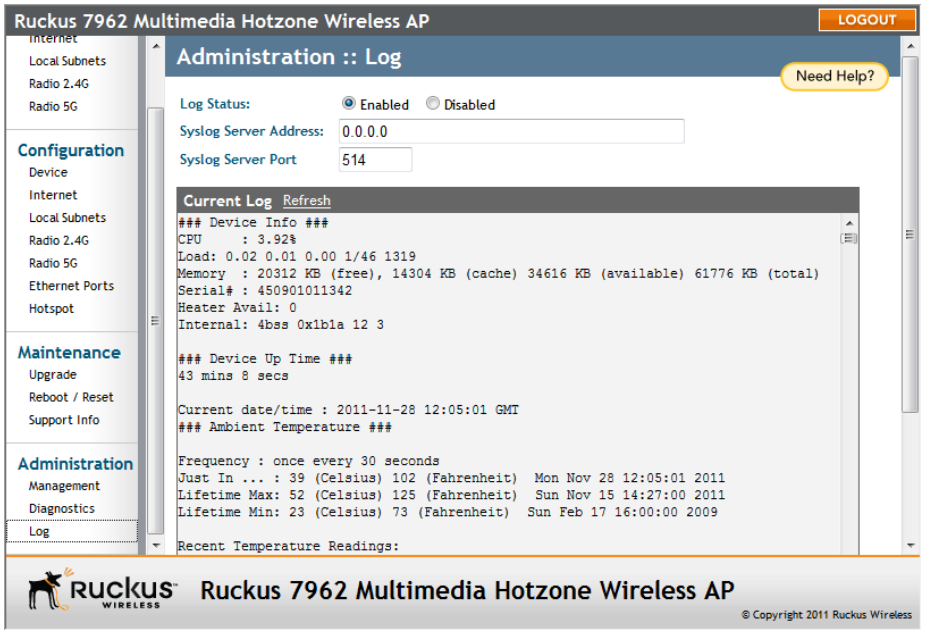
Both the *Maintenance* > *Support Info* and *Administration* > *Log* pages can be used to view the AP's current log file text. You can use the former to send the log to Ruckus Wireless support directly or save it to a local file, and use the latter to configure automatic delivery of log files to a syslog server.

Enabling Logging and Sending Event Logs to a Syslog Server

If you have a syslog server on the network, you can configure the Access Point to send the device logs to the server. You will need to enable logging (if disabled) and configure the Access Point to send logs to the syslog server.

1. Go to **Administration** > **Log**. The Administration > Log page appears.
2. Look for **Log Status,** and then click **Enabled**.
3. After enabling logging, configure the following options:
   - **Syslog Server Address**: To enable the AP to send messages to a syslog server as they appear, enter the IP address of the syslog server.
   - **Syslog Server Port**: By default, the syslog port number is 514. If the syslog server is using a different port, enter that port number in this field.
4. Click **Update Settings** to save and apply your changes.

Figure 51. The Administration > Log page



Sending a Copy of the Log File to Ruckus Wireless Support

The Support Info log consists of the configuration and run-time status of the AP and can be useful for troubleshooting. You have three options for sending a copy of the current log file to Ruckus Wireless Support:

- Save a copy to your local PC, then attach it to an e-mail message and send it to support
- Set up a connection to an FTP site
- Set up a connection to a TFTP site

To take advantage of these options

1. Go to **Maintenance** > **Support Info**. The Maintenance > Support Info page appears.
2. Review the Upload Method options.
3. To upload a copy of the support info file to an FTP or TFTP server, click the TFTP or FTP option. Clicking the FTP option prompts you to enter a User ID and Password.
4. In **Server Address**, enter the FTP or TFTP server IP address.
5. In **Filename**, enter a name for this file that you are saving.

NOTE: Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host."

6. Click **Upload Now**.

Saving a Copy of the Current Log to Your Computer

You can also save a copy of the current log to your own computer, if needed.

1. Go to **Maintenance** > **Support Info**. The Maintenance > Support Info workspace appears.
2. Review the Upload Method options
3. Click the **Save to local computer** option. Two links appear next to **Download** (*supportinfo.txt* and *tr069info.txt*).
4. Click the **supportinfo.txt** link. A new window (or tab) opens with the content of the log file displayed.
5. Choose **Save As** or **Save Page As** from your browser's **File** menu.
6. When the "Save as..." dialog box appears, find a convenient location on your local computer to save the file, and change the file extension from *html* to *txt*.
7. Click **Save** to save the file to your computer.

Upgrading the Firmware

You can use the Web interface to check for software updates/upgrades for the firmware built into the AP. You can then apply these updates to the device in one of two ways: (1) manual updating on an as-needed basis or (2) automating a regularly scheduled update.

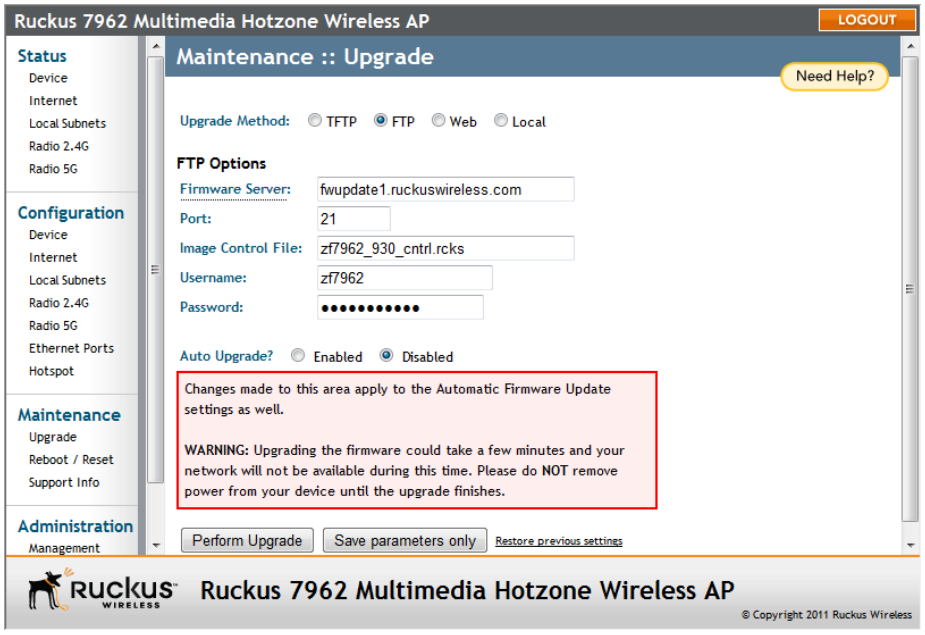
Before starting, decide which option you want to take:

- Automate a regularly scheduled update
- Run a one-time manual update right now

By default, the automatic upgrade option is disabled.

To get started with upgrading the firmware, go to **Maintenance** > **Upgrade**. When the **Maintenance** > **Upgrade** options appear, decide which upgrade method to use. Each of the upgrade options listed on the Upgrade page are discussed in the succeeding sections.

Figure 52. The Maintenance > Upgrade page



Upgrading Manually via FTP or TFTP

1. In the **Upgrade Method** options, click **FTP** or **TFTP**.
2. Click the host name field, and then type the URL of the server. Or click the IP address field, and then type the IP address of the server. Remember to start the URL with `ftp://`.

CAUTION: Do not change any of the Image Control File, Username, or Password entries.

3. Click **Perform Upgrade**. A status bar appears during the upgrade process.
4. After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via the Web

1. In the **Upgrade Method** options, click **Web**.
2. If instructed to choose a different URL than the default value, click the **Web Options URL** field, and then type the URL of the download Web site. Remember to start the URL with "http://".
3. Click **Perform Upgrade**. A status bar appears during the upgrade process.
4. After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via Local File

If you have already saved a firmware file on your local computer, you can upgrade directly using the Web interface.

1. In the **Upgrade Method** options, choose **Local**.
2. Click the **Browse** button and locate the file on your local computer.
3. Select the file and click **OK**.
4. Click **Perform Upgrade**. A status bar appears during the upgrade process.
5. After the upgrade is completed, you must manually reboot the AP.

Scheduling Automatic Upgrades

1. In the Upgrade Method options, click the button for your preferred choice.
2. Enter the appropriate information in the Host name field or IP address field.

CAUTION: Do not change any of the Image Control File, Username, or Password entries.

3. Verify that the Auto Upgrade option is set to **Enabled**.
4. Toggle the **Interval to Check for Software Upgrade** drop-down list to select your preferred interval.

5. Choose whether to reboot immediately after upgrading, or schedule the reboot for a specific time of day using the **Schedule Reboot Time After Upgrade** list. Choosing **Any Time** (the default value) results in the AP performing a reboot immediately after the automatic upgrade is successful.
6. You have two options at this point:
   - Click **Perform Upgrade**, which will start the process and the clock. The next upgrade will occur at the selected interval.
   - Click **Save parameters only**. The clock starts right away, and the actual upgrade will occur at the first effective interval.

   After you click one of these two options, a status bar appears during the upgrade process.

When the upgrade is complete, the AP will reboot automatically at the time you specified in step 5.

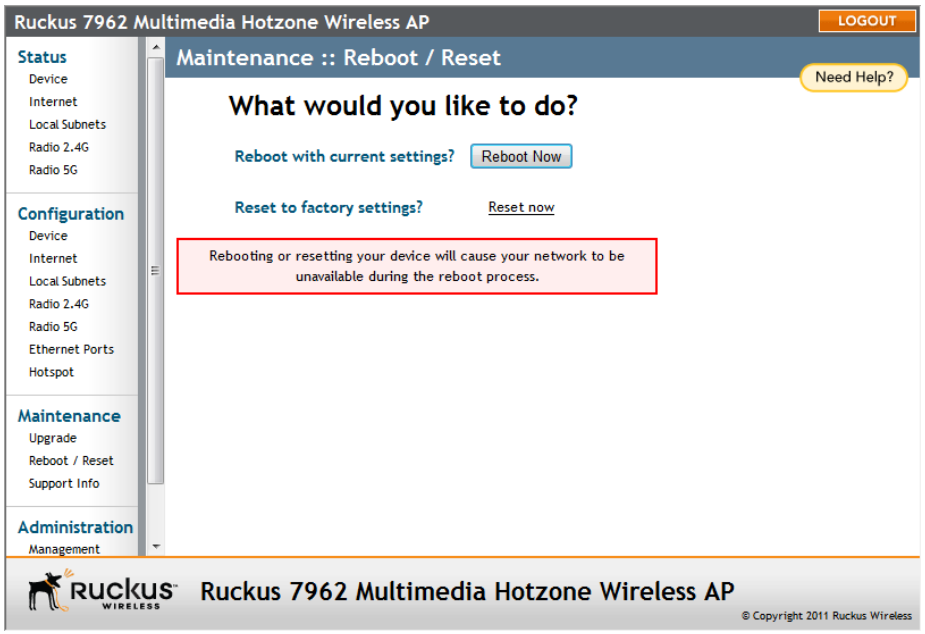
Rebooting the Access Point

You can use the Web interface to prompt the AP to reboot, which simply restarts the AP without changing any of the current settings. Please note that rebooting the AP will disrupt network communications in any currently active WLANs.

To reboot the Access Point

1. Go to **Maintenance** > **Reboot/Reset**. The Maintenance > Reboot/Reset page appears.
2. Click **Reboot Now**. After a brief pause, you will be automatically logged out of the AP.

Figure 53. The Maintenance > Reboot/Reset page



After approximately one minute, you should be able to log back into the AP, which verifies that the reboot was successful. You can also check the LEDs on the AP to verify the status of the device.

Resetting the Access Point to Factory Defaults

WARNING: DO NOT reset the Access Point to factory defaults unless you are directed to do so by Ruckus Wireless support staff or by a network administrator. Do this only if you are able to immediately reconnect the restored AP to your computer, to reconfigure it for Wi-Fi network use — as detailed in "Installing the Access Point" on page 21.

You can use the Web User interface to restore an inoperative AP to its factory default settings, which will completely erase the configuration currently active in the device. Note, too, that this will disrupt all wireless network communications through this device.

To reset the Access Point to factory defaults

1. Go to **Maintenance** > **Reboot/Reset**. The Maintenance > Reboot/Reset page appears.

2. Click **Reset Now** (next to *Restore to factory settings*?).
3. When the confirmation warning appears, read the message and click **OK** if you are certain that you want to restore the AP to factory defaults.

After a brief pause, you will be automatically logged out of the AP. You must now disconnect the AP from the switch (and the network) and reconnect it to your computer, as described in "Step 1: Preconfigure the Access Point" on page 28. At this time, you can restore the network settings, then replace it in your site for full network use.

Running Diagnostics

Two network connection diagnostic tools – PING and traceroute – have been built into the AP to help you check network connections from the Web interface.

To run diagnostics for network troubleshooting

1. Go to **Administrator** > **Diagnostics**. The Administrator > Diagnostics page appears. Two options are available:
   - Ping
   - Traceroute
2. Click the text field by the option you want to activate, and type the network address of a site you wish to connect to.
3. Click **Run Test**.

The results appear in the text field below each option.

Figure 54. Pinging a client

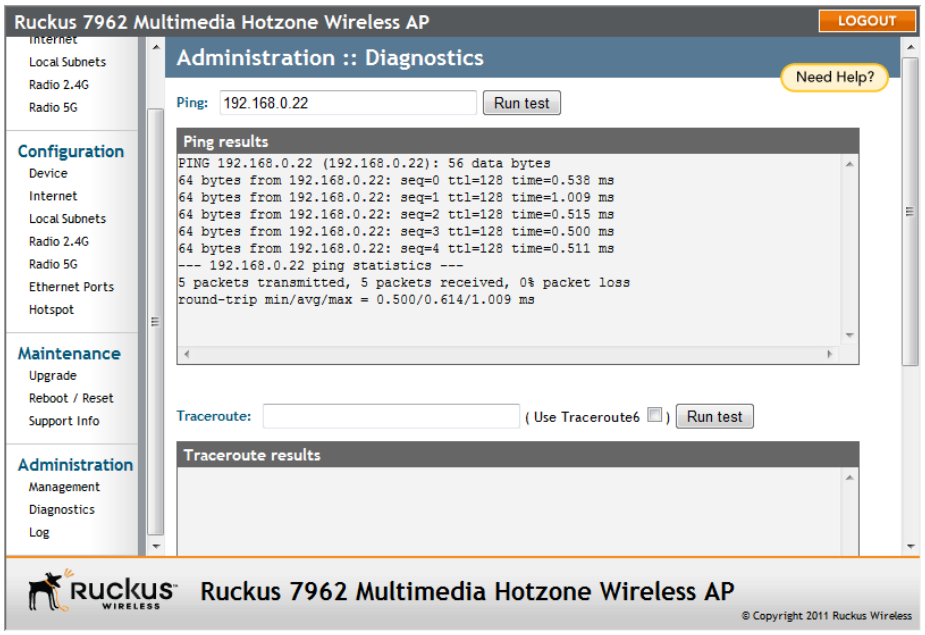
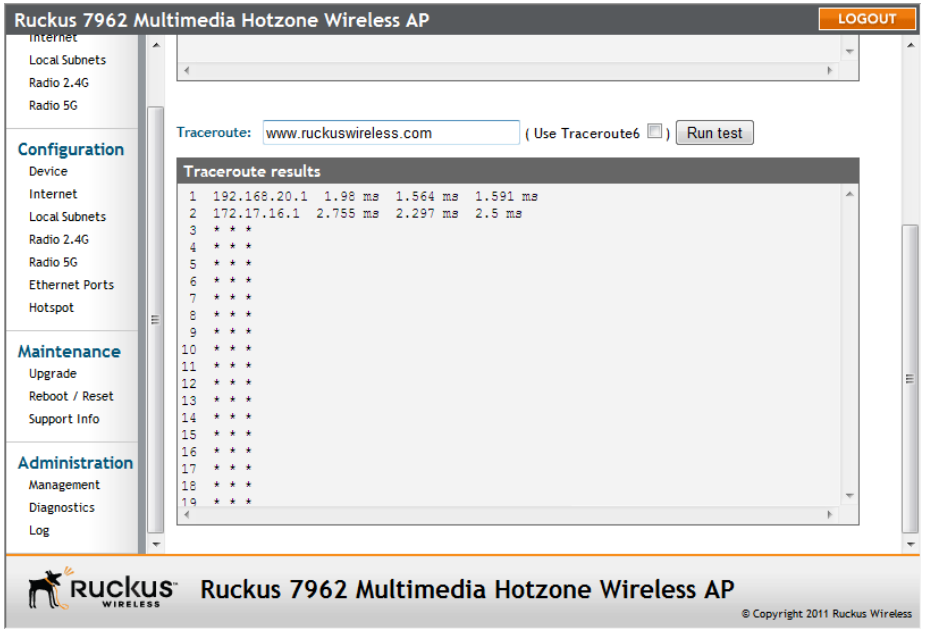


Figure 55. Running traceroute on ruckuswireless.com



Where to Find More Information

If you have questions that this User Guide does not address, visit the Ruckus Wireless Support Portal at http://support.ruckuswireless.com/. The Support Portal hosts the latest versions of user documentation. You can also find answers to frequently asked questions (FAQs) for each Ruckus Wireless product type.

Index

Numerics

802.1X, 69, 76, 78
802.1X settings, 69

A

access control, 72–73
Access Port, 76–77
Access VLAN, 64
administrative login, 93
AeroScout, 58
associated clients, 92
auto discovery, 28

B

BeamFlex, 1
Bridge to L2TP Tunnel, 63, 76
Bridge to WAN, 63, 76
broadcast SSID, 63

C

changing the login settings, 48
country code, 58, 91

D

default IP address, 50
default user name and password, 43
device location, 48
device name, 48
device settings, 48
DHCP
  release, 51
  renew, 51
DHCP Option 82, 64, 77
diagnostics, 106
disable Ethernet ports, 75
Dynamic VLAN, 64

E

encryption, 64
Ethernet ports
  configuration, 75

F

firmware upgrade, 102
FlexMaster, 1, 30
FlexMaster management status, 98
FlexMaster server address, 35

G

General Port, 76, 78

H

Help, 45
Hotspot
  basic settings, 80
  network settings, 86
  optional settings, 82
  unrestricted access, 85
  walled garden, 84

I

installation, 21
  required tools, 21
Internet settings, 49
IP address, 50
Isolated, 63, 76

K

Kensington lock, 9

L

L2TP, 53

Local Bridging, 76
local subnet, 64
Local Subnet NAT and Route to WAN, 63, 76
local subnets, 55
location, 23
lock hasp, 10
logging in, 43
logout, 44

M

MAC authentication bypass, 79
management access options, 94
Management VLAN, 50
menu, 44
mounting recommendations, 23

N

NTP Server, 50

O

optimal mounting, 23
orientation, 23

P

package contents, 2
packet forwarding, 63, 76
ping, 106
Port Type, 76
port-based VLAN, 75, 80
protection mode, 61

R

rebooting, 104
releasing DHCP, 51
renewing DHCP, 51
resetting to factory default, 105
router mode, 55

S

site survey, 22
SSID, 63
standalone operation, 30
syslog, 100

T

tabs, 44
temperature update, 48
threshold, 63
traceroute, 106
transmit power, 61
Trunk Port, 76–77
Tunnel via L2TP, 63, 76

U

user name, 48

V

verifying operation, 37
viewing associated clients, 92
VLAN, 75, 77
  overview, 49
  wired, 80
  wireless, 64

W

Web interface, 43
WEP, 64
wireless availability, 63
wireless channel, 58, 91
wireless mode, 58, 91
wireless security
  802.11X, 69
  WEP, 64
  WPA, 66
wireless settings, 56
workspace, 44
WPA, 66
WPA-Auto, 68

Z

ZoneDirector, 1, 28
ZoneFlex 2942/7942, 3
  LEDs, 3
  rear panel, 5
  side panel, 3

ZoneFlex 7341, 11
ZoneFlex 7341/7343/7363
  Front Panel, 11, 13, 17
  Rear Panel, 13, 16, 19
ZoneFlex 7343, 13
ZoneFlex 7363, 17
ZoneFlex 7962, 7
  LEDs, 7
  rear panel, 10
  side panel, 7
ZoneFlex smart WLAN system, 1